

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Masaki KYOJIMA, Kil-ho SHIN

Application No.: New U.S. Patent Application

Filed: October 3, 2000

Docket No.: 107500

For: LICENSE-ISSUING SYSTEM AND METHOD

**CLAIM FOR PRIORITY**

Director of the U.S. Patent and Trademark Office  
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2000-024525 filed February 2, 2000

In support of this claim, a certified copy of said original foreign application:

  X   is filed herewith.

           was filed on            in Parent Application No.            filed           .

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

*James A. Oliff*

James A. Oliff  
Registration No. 27,075

Thomas J. Pardini  
Registration No. 30,411

JAO:TJP/cmm  
Date: October 3, 2000

**OLIFF & BERRIDGE, PLC**  
**P.O. Box 19928**  
**Alexandria, Virginia 22320**  
**Telephone: (703) 836-6400**

**DEPOSIT ACCOUNT USE  
AUTHORIZATION**  
Please grant any extension  
necessary for entry;  
Charge any fee due to our  
Deposit Account No. 15-0461

10925 U.S. PTO  
09/678031  
10/03/00

日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT

JC925 U.S. PTO

09/678031



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
in this Office.

出願年月日

Date of Application:

2000年 2月 1日

願番号

Application Number:

特願2000-024525

願人

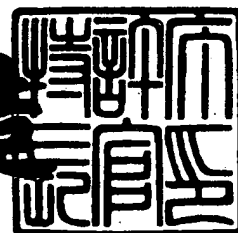
Applicant(s):

富士ゼロックス株式会社

2000年 7月21日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 FE00-00025

【提出日】 平成12年 2月 1日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/00

【発明の名称】 利用許可証発行装置および方法

【請求項の数】 31

【発明者】

【住所又は居所】 神奈川県足柄上郡中井町境4 3 0 グリーンテクなかい  
富士ゼロックス株式会社内

【氏名】 京嶋 仁樹

【発明者】

【住所又は居所】 神奈川県足柄上郡中井町境4 3 0 グリーンテクなかい  
富士ゼロックス株式会社内

【氏名】 申 吉浩

【特許出願人】

【識別番号】 000005496

【氏名又は名称】 富士ゼロックス株式会社

【電話番号】 0462-38-8516

【代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 038818

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 利用許可証発行装置および方法

【特許請求の範囲】

【請求項 1】 デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行する方法であって、

利用許可証の正当性を検証するために必要な検証用情報を作成するステップと、

検証用情報を特定するための情報を入力するステップと、

入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な利用許可証を作成するステップと、

作成された利用許可証を出力するステップと

を備えていることを特徴とする利用許可証発行方法。

【請求項 2】 デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行するコンピュータシステムであって、

利用許可証の正当性を検証するために必要な検証用情報を作成する検証用情報作成手段と、

上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、

検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な利用許可証を作成する利用許可証作成手段と、

上記利用許可証作成手段で作成された利用許可証を出力する利用許可証出力手段と

を備えることを特徴とする利用許可証発行システム。

【請求項 3】 デジタルコンテンツの利用を限定するための条件である利用条件を作成する利用条件作成手段を備え、

上記利用許可証作成手段が作成した利用許可証に、上記利用条件作成手段が作成した利用条件が含まれていることを特徴とする

請求項 2 記載の利用許可証発行システム。

【請求項 4】 利用許可証作成手段が、

検証用情報を特定するための情報とともに、利用許可証発行の仲介者を特定するための情報と、該特定される検証用情報に対応する利用許可証の発行の仲介が該特定される仲介者に許諾されていることを証明する利用許可証仲介許諾証が入力され、

利用許可証仲介許諾証によって該仲介者に該検証用情報に対応する利用許可証の発行の仲介が許諾されているかを確認し、許諾されている場合にのみ利用許可証を作成することを特徴とする

請求項 2 記載の利用許可証発行システム。

【請求項 5】 利用許可証の発行履歴を記憶する利用許可証発行履歴記憶部と、

デジタルコンテンツの提供者を特定するための情報の入力を受け、利用許可証発行履歴記憶部に記憶されている発行履歴から、該提供者が提供するデジタルコンテンツに関する利用許可証の発行履歴である利用許可証提供者用発行履歴を抽出する利用許可証提供者用発行履歴作成部と、

前記利用許可証提供者用発行履歴作成部で作成された利用許可証提供者用発行履歴を出力する利用許可証提供者用発行履歴出力部とをさらに備えることを特徴とする

請求項 2 記載の利用許可証発行システム。

【請求項 6】 さらに、利用許可証の発行の依頼を受理する利用許可証発行依頼受理手段を備え、

上記利用許可証発行依頼受理手段が利用許可証発行依頼を受理した場合に、利用許可証作成手段で利用許可証を作成し、

利用許可証の発行履歴を記憶する利用許可証発行履歴記憶部と、

利用許可証発行の依頼者を特定するための情報の入力を受け、利用許可証発行履歴記憶部に記憶されている発行履歴から、該依頼者から依頼された利用許可証の発行履歴である利用許可証依頼者用発行履歴を抽出する利用許可証依頼者用発行履歴作成部と、

前記利用許可証依頼者用発行履歴作成部で作成された利用許可証依頼者用発行

履歴を出力する利用許可証依頼者用発行履歴出力部とをさらに備えることを特徴とする

請求項 2 記載の利用許可証発行システム。

【請求項 7】 検証用情報の発行履歴を記憶する検証用情報発行履歴記憶部と、

検証用情報の被発行者を特定するための情報の入力を受け、検証用情報発行履歴記憶部に記憶されている発行履歴から、該被発行者に対して発行された検証用情報に関する検証用情報の発行履歴である検証用情報発行被発行者用履歴を抽出する検証用情報発行履歴作成部と、

前記検証用情報発行履歴作成部で作成された検証用情報発行被発行者用履歴を出力する検証用情報発行履歴出力部とをさらに備えることを特徴とする

請求項 2 記載の利用許可証発行システム。

【請求項 8】 さらに、公開鍵暗号ペアを作成する公開鍵暗号ペア作成手段と、

上記公開鍵暗号ペア作成手段で作成された公開鍵ペアのうちの秘密鍵を保持する秘密鍵保持手段とを備え、

検証用情報が上記公開鍵暗号ペア作成手段で作成された公開鍵であり、  
利用許可証が秘密鍵保持手段に保持されている秘密鍵を使用して作成されることを特徴とする

請求項 2 記載の利用許可証発行システム。

【請求項 9】 デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼を仲介する方法であって、

特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第 1 の利用許可証依頼を受領するステップと、

受領した第 1 の利用許可証依頼で依頼されている利用許可証の発行を依頼する第 2 の利用許可証依頼を作成するステップと、

作成された第 2 の利用許可証依頼を出力するステップと

を有することを特徴とする利用許可証仲介方法。

【請求項 10】 デジタルコンテンツの利用が特定のユーザに対して許可さ

れていることを証明する電子的な利用許可証の依頼を仲介するコンピュータシステムであって、

特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第 1 の利用許可証依頼を受領する利用許可証依頼受領手段と、

受領した第 1 の利用許可証依頼で依頼されている利用許可証の発行を依頼する第 2 の利用許可証依頼を作成する利用許可証依頼作成手段と、

上記利用許可証依頼作成手段で生成された第 2 の利用許可証依頼を出力する利用許可証依頼出力手段と

を有することを特徴とする利用許可証仲介システム。

【請求項 1 1】 特定の利用許可証の正当性を検証するために必要な検証用情報が特定のデジタルコンテンツに対応づけられており、

第 1 および第 2 の利用許可証依頼に、該依頼が利用許可証を依頼するデジタルコンテンツを特定するために検証用情報を特定するための情報が含まれる

ことを特徴とする請求項 1 0 記載の利用許可証仲介システム。

【請求項 1 2】 依頼する利用許可証がデジタルコンテンツの利用を限定するための条件である利用条件を含むものであり、

依頼する利用許可証に含まれるべき利用条件を作成する利用条件作成手段を備え、

利用許可証依頼作成手段が作成した第 2 の利用許可証依頼に、上記利用条件作成手段が作成した利用条件が含まれることを特徴とする

請求項 1 0 記載の利用許可証仲介システム。

【請求項 1 3】 自らが特定のデジタルコンテンツに対する利用許可証の発行の仲介を許諾されていることを証明する利用許可証仲介許諾証を保持する利用許可証仲介許諾証記憶手段を備え、

利用許可証依頼出力手段が作成する利用許可証依頼に、利用の対象となるデジタルコンテンツに対するものであり、かつ、利用許可証仲介許諾証記憶手段に保持されている利用許可証仲介許諾証を添付することを特徴とする

請求項 1 0 記載の利用許可証仲介システム。

【請求項 1 4】 さらに、第 1 の利用許可証依頼の依頼者に利用許可証発行



料金の課金を行う課金手段を備え、

第 1 の利用許可証を受領した時に、上記課金手段によって所定の利用許可証発行料金を該依頼者に対して課金することを特徴とする

請求項 1 0 記載の利用許可証仲介システム。

【請求項 1 5】 さらに、第 1 の利用許可証依頼の依頼者から利用許可証発行料金を徴収する決済手段を備え、

第 1 の利用許可証依頼を受領した時に、上記決済手段によって所定の利用許可証発行料金を該依頼者から徴収することを特徴とする

請求項 1 0 記載の利用許可証仲介システム。

【請求項 1 6】 デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾する方法であって、

デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報を入力するステップと、

該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報を入力するステップと、

入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成するステップと、

作成された利用許可証仲介許諾証を出力するステップとを有することを特徴とする利用許可証仲介許諾方法。

【請求項 1 7】 デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾するコンピュータシステムであって、

デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報とが入力され、入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成する利用許可証仲介許諾証作成手段と、

上記利用許可証仲介許諾証作成手段で作成された利用許可証仲介許諾証を出力する利用許可証仲介許諾証出力手段と

を有することを特徴とする利用許可証仲介許諾システム。

【請求項 1 8】 許諾証の受け手である仲介者が仲介することで発行される利用許可証に記載される利用を限定するための条件である利用条件の範囲を限定するための情報である利用条件限定情報を作成する利用条件限定情報作成手段を備え、

上記利用許可証仲介許諾証作成手段が作成した利用許可証仲介許諾に、上記利用条件限定情報作成手段が作成した利用条件限定情報が含まれていることを特徴とする

請求項 1 7 記載の利用許可証仲介許諾システム。

【請求項 1 9】 許諾証の発行履歴を記憶する利用許可証仲介許諾証発行履歴記憶部と、

利用許可証の依頼の仲介者を特定するための情報の入力を受け、利用許可証仲介許諾証発行履歴記憶部に記録されている発行履歴から、該仲介者に対して発行された許諾証に関する履歴である利用許可証仲介許諾証発行仲介者用履歴を抽出する利用許可証仲介許諾証発行仲介者用履歴作成部と、

前記利用許可証仲介許諾証発行仲介者用履歴作成部で作成された利用許可証仲介許諾証発行仲介者用履歴を出力する利用許可証仲介許諾証発行仲介者用履歴出力部とをさらに備えることを特徴とする

請求項 1 7 記載の利用許可証仲介許諾システム。

【請求項 2 0】 ユーザに一つ以上の機能を提供する方法であって、すべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、

利用許可証を入力するステップと、

入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、

入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能

のうち少なくとも一部を動作可能にするステップと  
を含む事の特徴とする機能提供方法。

【請求項 2 1】 デジタルコンテンツを操作する方法であって、  
デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明  
する電子的な利用許可証を検証するための検証用情報を記憶するステップと、  
利用許可証を入力するステップと、  
入力された利用許可証の正当性を記憶されている検証用情報を使用して検証す  
るステップと、  
入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツ  
に対する操作のうちの少なくとも一部を動作可能にするステップと  
を含む事の特徴とするデジタルコンテンツ操作方法。

【請求項 2 2】 暗号化されたデジタルコンテンツを復号する方法であって、  
デジタルコンテンツの復号が特定のユーザに対して許可されていることを証明  
する電子的な利用許可証を検証するための検証用情報を記憶するステップと、  
利用許可証を入力するステップと、  
入力された利用許可証の正当性を記憶されている検証用情報を使用して検証す  
るステップと、  
入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタル  
コンテンツを復号するステップと  
を含む事の特徴とするデジタルコンテンツ復号方法。

【請求項 2 3】 圧縮されたデジタルコンテンツを伸長する方法であって、  
デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明  
する電子的な利用許可証を検証するための検証用情報を記憶するステップと、  
利用許可証を入力するステップと、  
入力された利用許可証の正当性を記憶されている検証用情報を使用して検証す  
るステップと、  
入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタル  
コンテンツを伸長するステップと

を含む事の特徴とするデジタルコンテンツ伸長方法。

【請求項 2 4】 ユーザに一つ以上の機能を提供する装置であって、  
該装置のすべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能のうち少なくとも一部を動作可能にすること  
を特徴とする装置。

【請求項 2 5】 デジタルコンテンツを操作する装置であって、  
デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツに対する操作のうちの少なくとも一部を動作可能にすること

を特徴とするデジタルコンテンツ操作装置。

【請求項 2 6】 該検証用情報がデジタルコンテンツに含まれており、  
該検証用情報をデジタルコンテンツから取り出して、該検証用情報記憶手段に記憶する

ことを特徴とする請求項 2 5 記載のデジタルコンテンツ操作装置。

【請求項 2 7】 暗号化されたデジタルコンテンツを復号する装置であって  
デジタルコンテンツの復号が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを復号すること  
を特徴とするデジタルコンテンツ復号装置。

【請求項 2 8】 該検証用情報が暗号化されたデジタルコンテンツに含まれており、

該検証用情報を暗号化されたデジタルコンテンツから取り出して、該検証用情報記憶手段に記憶する

ことを特徴とする請求項 2 7 記載のデジタルコンテンツ復号装置。

【請求項 2 9】 圧縮されたデジタルコンテンツを伸長する装置であって、伸長の対象となる圧縮されたデジタルコンテンツを入力する手段と、

デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを伸長すること  
を特徴とするデジタルコンテンツ伸長装置。

【請求項 3 0】 該検証用情報が圧縮されたデジタルコンテンツに含まれており、

該検証用情報を圧縮されたデジタルコンテンツから取り出して、該検証用情報記憶手段に記憶する

ことを特徴とする請求項 2 9 記載のデジタルコンテンツ伸長装置。

【請求項 3 1】 さらに、利用許可証を保持している携帯用記憶装置を接続する接続手段を備え、

利用許可証検証手段が、上記接続手段を通して接続された携帯用記憶装置に記憶されている利用許可証の正当性を検証することを特徴とする

請求項 2 4 ～ 3 0 のいずれかに記載の利用許可証検証装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンピュータシステムにおいてデジタルコンテンツの利用を許可する技術に関わり、特に、ユーザがデジタルコンテンツの利用を許可されていることを証する利用許可証の発行や、該利用許可証の正当性の検証に関する。

【0 0 0 2】

【従来の技術】

インターネットの急速な普及に伴い、画像、音声、映像といったデジタルデータあるいはソフトウェアといったデジタルコンテンツをインターネット経由で提供し、対価を得るというビジネスが広がりつつある。デジタルコンテンツの提供者の立場にたてば、インターネットを利用すれば、デジタルコンテンツのパッケージングや流通のためのコストを省くことができるというメリットがあり、また、消費者からみれば、家庭にいながらもデジタルコンテンツを入手できるというメリットがある。インターネット経由のデジタルコンテンツの提供は、今後、デジタルコンテンツを対象としたビジネスの主流になっていくことは疑いない。

【0 0 0 3】

現在のデジタルコンテンツの販売において最も問題なのは、デジタルコンテンツの利用者から正しく対価を徴収するのが困難なことである。最近では、電子的な決済手段が整い始め、金銭の授受自体は安全に行えるようになりつつある。したがって、デジタルコンテンツの利用者に正しく対価を支払う意志がある限りは、問題が起こりにくくなってきた。しかし、何の痕跡もなく複製が可能であるというデジタルコンテンツの特徴により、対価を支払う意志のないものがコンテンツを複製し、使用することは非常に容易である。

【0 0 0 4】

この問題に関して、現在もっとも多く取られている方法が、サイトのアクセスコントロールである。

【0 0 0 5】

この方法では、消費者は、デジタルコンテンツをインターネット上にあるサイトからダウンロードする。そのサイトにはアクセスコントロールがかけてあり、対価を支払った消費者のみがデジタルコンテンツをダウンロードすることが可能である。サイトにアクセスした消費者からは対価が徴収できるものの、ダウンロードした後のデジタルコンテンツは複製が可能であり、その複製の利用者からは対価を得ることができないことが問題である。しかし、少なくともデジタルコンテンツをダウンロードした消費者からは対価が得られること、また、仕組みが簡便で導入しやすいことから、この方法を利用している業者は多い。

## 【 0 0 0 6 】

複製したデジタルコンテンツの利用者からかも対価を徴収するために考案された手段が、ソフトウェアキーと呼ばれる利用許可証を利用した方法である。主にソフトウェアの販売に利用される方法であり、シェアウェアの代金回収に用いられることが多い。

## 【 0 0 0 7 】

この方法では、デジタルコンテンツの提供者は、自己が提供するデジタルコンテンツに対して有効なソフトウェアキーと呼ばれるデジタルデータの集合と、そのソフトウェアキーの有効性を検証する方法とを決定する。デジタルコンテンツにはソフトウェアキーの検証方法が実装され、有効なソフトウェアキーが提示されたときにのみ、自己の利用を許すように作成される。ソフトウェアキーは、デジタルコンテンツの対価を払った消費者にのみ送付されるので、デジタルコンテンツを利用できるのはデジタルコンテンツの対価を支払った消費者のみとなる。逆にいえば、デジタルコンテンツを使用したい消費者は、デジタルコンテンツの提供者から必ずソフトウェアキーを購入しなければならない。

## 【 0 0 0 8 】

## 【発明が解決しようとする課題】

デジタルコンテンツの提供者が有効なソフトウェアキーの集合とそのソフトウェアキーの有効性を検証する方法とを決定する仕組みでは、ソフトウェアキーに関する開発コストや、ソフトウェアキーを販売・発行する運営コストをデジタルコンテンツの提供者が負わなければならない。ソフトウェアキーは、デジタルコ

ンテンツに対する消費者の利用権を証する利用許可証ともいえるデジタルデータであり、漏洩、偽造、複製といったセキュリティ上の様々な問題に対する耐性が必要となる。このような仕組みの開発や運営はコストの上昇をもたらし、デジタルコンテンツの提供者がこのソフトウェアキーを利用したデジタルコンテンツのオンライン販売に乗り出す際の重大な障壁になるとともに、販売価格の上昇という不利益を消費者にもたらす。

## 【 0 0 0 9 】

## 【課題を解決するための手段】

本発明では、販売される特定のデジタルコンテンツあるいはデジタルコンテンツ提供者、あるいは、デジタルコンテンツ販売業者とは独立の利用許可証の発行を担うサーバ（以降、利用許可証発行センタあるいは単にセンタとよぶ）をインターネット上に構築することで、上記の課題を解決する。利用許可証の作成や維持に関わる部分は利用許可証発行センタがすべて引き受け、デジタルコンテンツの販売を行う業者は利用許可証に関わる部分の多くを利用許可証発行センタにアウトソーシングすることができる。多くの業者が共通の利用許可証発行センタを使用することが可能なので、業者一つあたりの利用許可証発行センタの開発・運営コストは業者が独自のシステムを構築するのにくらべて低く押さえることができる。

## 【 0 0 1 0 】

本発明では、デジタルコンテンツ販売業者は、消費者から受けたデジタルコンテンツの購入依頼に対して利用許可証を発行するが、その利用許可証は利用許可証発行センタで生成される。該業者は、消費者からの購入依頼を受け付けるサーバをインターネット上に構築するが、許可証を生成する部分は該サーバ中には存在せず、利用許可証発行センタがその役割を担う。

## 【 0 0 1 1 】

デジタルコンテンツの利用時には、消費者は利用許可証を提示し、利用許可証の正当性が確認されたときにのみコンテンツの利用が可能になるが、この検証は検証用情報と呼ばれるデジタルデータを使用して行われる。検証用情報は複数の利用許可証との間に所定の関係を満たすように生成されており、検証用情報と利



用許可証がその関係を満たすかどうかで利用許可証の正当性が判定される。特定のデジタルコンテンツと特定の検証用情報をバインドさせておけば、その検証用情報と所定の関係を満たす利用許可証を提示できるかどうかで、消費者がデジタルコンテンツを購入したかどうか判定できる。

## 【 0 0 1 2 】

検証用情報は、センタで生成され出力される。どの業者が販売した利用許可証であっても対応する検証用情報を入手していればその正当性を検証することが可能である。

## 【 0 0 1 3 】

この特徴は、デジタルコンテンツの販売ビジネスに乗り出す業者が払うべきコストを更に下げる効果を持つ。本発明では、デジタルコンテンツの提供者と、それらの販売業者は互いに独立に存立できる。デジタルコンテンツの提供者は、自分が提供するデジタルコンテンツの販売を多くの販売業者に委託し、自己はデジタルコンテンツの提供に専念することができる。また、販売業者は、自らが提供するデジタルコンテンツをまったく持たなくても、様々な提供者が提供する多くのデジタルコンテンツを販売する事が可能である。

## 【 0 0 1 4 】

請求項 1 または 2 に記載の発明は利用許可証発行センタに関するものである。

## 【 0 0 1 5 】

請求項 1 に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行する方法であって、利用許可証の正当性を検証するために必要な検証用情報を作成するステップと、検証用情報を特定するための情報が入力するステップと、入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な利用許可証を作成するステップと、作成された利用許可証を出力するステップとを備える。

## 【 0 0 1 6 】

また、請求項 2 に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行するコンピュータシステムであって、利用許可証の正当性を検証するために必要な検証用情報を

作成する検証用情報作成手段と、上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な利用許可証を作成する利用許可証作成手段と、上記利用許可証作成手段で作成された利用許可証を出力する利用許可証出力手段とを備える。

## 【0017】

請求項1または2に記載の発明によるセンタは、利用許可証を発行するだけでなく、利用許可証を検証するための検証用情報も出力する。この検証用情報はデジタルコンテンツの利用の際に消費者から提示される利用許可証の正当性を検証する際に使用される。特定の検証用情報によって検証可能な利用許可証の集合は限定されるので、特定のデジタルコンテンツの検証用情報を割り当てることで、デジタルコンテンツ毎の利用許可証の発行が可能である。しかし、どの検証用情報（あるいはそれに対応する利用許可証の集合）がどのデジタルコンテンツに対応するかに関してセンタは関与する必要はない。デジタルコンテンツと検証用情報との連結はデジタルコンテンツの提供者が自由に決定することができる。このことが、利用許可証発行センタを、特定のデジタルコンテンツに関与しない利用許可証の発行にのみ特化したインフラストラクチャたらしめることを可能にする。

## 【0018】

請求項9または10に記載の発明は、デジタルコンテンツの販売を行うサーバに関するものである。

## 【0019】

請求項9に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼を仲介する方法であって、特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第1の利用許可証依頼を受領するステップと、受領した第1の利用許可証依頼で依頼されている利用許可証の発行を依頼する第2の利用許可証依頼を作成するステップと、作成された第2の利用許可証依頼を出力するステップとを有することを特徴とする。

## 【 0 0 2 0 】

また、請求項 1 0 に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼を仲介するコンピュータシステムであって、特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第 1 の利用許可証依頼を受領する利用許可証依頼受領手段と、受領した第 1 の利用許可証依頼で依頼されている利用許可証の発行を依頼する第 2 の利用許可証依頼を作成する利用許可証依頼作成手段と、上記利用許可証依頼作成手段で生成された第 2 の利用許可証依頼を出力する利用許可証依頼出力手段とを有することを特徴とする。

## 【 0 0 2 1 】

請求項 9 または 1 0 に記載の発明を適用した、デジタルコンテンツの販売を行うサーバは、インターネットに接続している消費者あるいは他の販売業者からの利用許可証発行の依頼を受けつける。しかし、受け付けた依頼に対する利用許可証を作成するのはこのサーバではない。利用許可証の発行は利用許可証発行センタのみが行い、デジタルコンテンツの販売を行うサーバは、利用許可証に対する依頼の仲介のみを行う。該サーバが行うのは、単に依頼の仲介のみであり、利用許可証の改竄、偽造、複製といった攻撃に対する配慮はセンタが行うので、本実施例に基づいたデジタルコンテンツの販売を行うサーバの構築費用や運営コストは低く押さえられる。

## 【 0 0 2 2 】

請求項 1 6 または 1 7 に記載の発明は、デジタルコンテンツの提供者に関するものである。

## 【 0 0 2 3 】

デジタルコンテンツの提供者と販売業者が独立に存立した場合、該提供者にとっては、自己が提供するデジタルコンテンツをより多くの販売業者に販売をしてもらうほうが、基本的には有利である。しかし、信頼できない販売業者に自己のデジタルコンテンツを扱われることは、後のトラブルを招く恐れが高く許容できない。したがって、デジタルコンテンツの提供者が、自己のデジタルコンテンツを扱える販売業者を限定できる手段が必要になる。

## 【 0 0 2 4 】

請求項 1 6 に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾する方法であって、デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報を入力するステップと、該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報を入力するステップと、入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成するステップと、作成された利用許可証仲介許諾証を出力するステップとを有することを特徴とする。

## 【 0 0 2 5 】

また、請求項 1 7 に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾するコンピュータシステムであって、デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報とが入力され、入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成する利用許可証仲介許諾証作成手段と、上記利用許可証仲介許諾証作成手段で作成された利用許可証仲介許諾証を出力する利用許可証仲介許諾証出力手段とを有することを特徴とする。

## 【 0 0 2 6 】

請求項 1 6 または 1 7 に記載の発明によれば、デジタルコンテンツの提供者は、自己が提供するデジタルコンテンツの販売を許す販売業者に対して利用許可証仲介許諾証を発行する。この利用許可証仲介許諾証は、販売業者が利用許可証の発行をセンタに依頼する場合にセンタに対して提示される。センタは提示された利用許可証仲介許諾証により、該販売業者が利用許可証の発行を依頼したデジタルコンテンツに対する仲介を許諾されているかどうかを検査することができる。

## 【 0 0 2 7 】

請求項 2 0 または 2 4 に記載の発明は、消費者に提供されるデジタルコンテンツ自体に関するものであり、とくに、消費者が自己を利用可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

## 【 0 0 2 8 】

請求項 2 0 に記載の発明は、ユーザに一つ以上の機能を提供する方法であって、すべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能のうち少なくとも一部を動作可能にするステップとを備える。

## 【 0 0 2 9 】

請求項 2 4 に記載の発明は、ユーザに一つ以上の機能を提供する装置であって、該装置のすべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能のうち少なくとも一部を動作可能にすることを特徴とする。

## 【 0 0 3 0 】

請求項 2 1 または 2 5 に記載の発明は、消費者に提供されるデジタルコンテンツを操作する装置あるいはソフトウェアに関するものであり、とくに、消費者がデジタルコンテンツを操作可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

## 【 0 0 3 1 】

請求項 2 1 に記載の発明は、デジタルコンテンツを操作する方法であって、デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許

可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツに対する操作のうちの少なくとも一部を動作可能にするステップとを備える。

## 【 0 0 3 2 】

請求項 2 5 に記載の発明は、デジタルコンテンツを操作する装置であって、デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツに対する操作のうちの少なくとも一部を動作可能にすることを特徴とする。

## 【 0 0 3 3 】

請求項 2 2 または 2 7 に記載の発明は、消費者に提供される暗号化されたデジタルコンテンツを復号する装置あるいはソフトウェアに関するものであり、とくに、消費者がデジタルコンテンツを復号可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

## 【 0 0 3 4 】

請求項 2 2 に記載の発明は、暗号化されたデジタルコンテンツを復号する方法であって、デジタルコンテンツの復号が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを復号するステップとを備える。

## 【 0 0 3 5 】

請求項 2 7 に記載の発明は、暗号化されたデジタルコンテンツを復号する装置であって、デジタルコンテンツの復号が特定のユーザに対して許可されているこ

とを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを復号することを特徴とする。

## 【 0 0 3 6 】

請求項 2 3 または 2 9 に記載の発明は、消費者に提供される圧縮されたデジタルコンテンツを伸長する装置あるいはソフトウェアに関するものであり、とくに、消費者がデジタルコンテンツを伸長可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

## 【 0 0 3 7 】

請求項 2 3 に記載の発明は、圧縮されたデジタルコンテンツを伸長する方法であって、デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを伸長するステップとを備える。

## 【 0 0 3 8 】

請求項 2 9 に記載の発明は、圧縮されたデジタルコンテンツを伸長する装置であって、伸長の対象となる圧縮されたデジタルコンテンツを入力する手段と、デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを伸長することを特徴とする。

## 【 0 0 3 9 】

なお、本発明はインターネットにおける利用に限定されるものではなく、広く

通信ネットワークに適用可能である。またネットワークにおける通信を利用せずに装置同志を用いて利用証明証を発行するようにしてもよいことはもちろんである。

#### 【0040】

##### 【発明の実施の形態】

以下に、本発明の一実施形態について説明する。

#### 【0041】

図1は本発明を適用した実施例の構成図である。本実施例は、インターネットに接続した複数のコンピュータシステムからなり、これらが協調して動作することでデジタルコンテンツの販売を行う。

#### 【0042】

本実施例では、消費者はデジタルコンテンツの購入をインターネット経由で行い、購入が完了したことを証するデジタルデータである利用許可証を受け取る。

#### 【0043】

デジタルコンテンツは、利用許可証を持つ消費者のみが利用可能なような形態で消費者に対して提供される。利用者は、利用許可証を所持している場合にのみ、デジタルコンテンツを使用することが可能である。

#### 【0044】

##### 【実施例を構成するコンピュータシステム群】

本実施例を構成するコンピュータシステムは以下の4つの種類に分類される。それぞれインターネット101に接続され、相互に通信を行う。

#### 【0045】

消費者端末：消費者がデジタルコンテンツの購入を行う際に使用するコンピュータシステム。図1の107にあたる。消費者が家庭で使用するコンピュータであってもよいし、コンビニエンスストア等に設置されている端末でもよい。インターネット101に接続されており、インターネット101経由で他のコンピュータシステムにアクセスすることができる。

#### 【0046】

リテーラ：消費者に対してデジタルコンテンツの販売を行うコンピュータシステ



ム。図1の103あるいは104にあたり、実際にはいくつ存在してもかまわない。インターネット101に接続されており、インターネット101経由で消費者からのアクセスを受け付ける。リテーラを運営しているのはデジタルコンテンツの販売をしている業者であるが、以降の本実施例の説明では、該コンピュータシステムと該業者を区別せず、ともにリテーラと呼ぶ事にする。

#### 【0047】

利用許可証発行センタ：利用許可証を生成し発行するコンピュータシステム。図1の102にあたる。インターネット101に接続されており、インターネット経由でリテーラからの利用許可証の依頼を受け付け、オンデマンドで利用許可証を作成し発行する。以降、センタといえは利用許可証発行センタを指す。

#### 【0048】

プロバイダ：デジタルコンテンツの提供者がリテーラ103あるいは104やセンタ102と情報の交換を行うためのコンピュータシステムであり、インターネット101に接続される。図1の105、106にあたり、実際にはいくつ存在してもかまわない。以降の本実施例の説明では、デジタルコンテンツの提供者と該提供者が使用するコンピュータシステムを区別せず、ともにプロバイダと呼ぶ事にする。

#### 【0049】

認証局 (Certificate Authority)：消費者端末、リテーラ、センタ、プロバイダのあいだで交わされる各メッセージには、改竄検知と否認拒否のためにデジタル署名が施される。そのデジタル署名の検証鍵の正当性はX. 509ベースの公開鍵証明証によって保証される。Certificate Authority 108はこの公開鍵証明証を作成し発行する機能を持つコンピュータシステムであり、インターネット101に接続されている。また、Certificate Authorityは、自己が発行した公開鍵証明証を保持しており、オンデマンドで要求者に送付する機能も持つ。以降、CAといえはCertificate Authorityを指す。

#### 【0050】

[利用許可証と検証用公開鍵]

本実施例では、消費者がデジタルコンテンツを購入したことを証明するために利用許可証と呼ばれるデジタルデータが発行される。利用許可証の正当性は対応する検証用公開鍵によって検証される。検証用公開鍵の名前が示すように、本実施例では利用許可証と検証用公開鍵には公開鍵暗号技術が応用される。

## 【 0 0 5 1 】

より具体的には、検証用公開鍵は公開鍵暗号における公開鍵であり、利用許可証は該公開鍵に対応する秘密鍵をもとに作成された証明値を含むデータである。利用許可証が含む証明値を作成する際に使用した秘密鍵と、検証用公開鍵が対応するものであった場合にのみ、利用許可証が正当なものであることが確認でき、それ以外の場合で利用許可証が正当なものであると認められることはない。

## 【 0 0 5 2 】

本実施例でデジタルコンテンツを販売する場合には、販売される特定のデジタルコンテンツあるいは、デジタルコンテンツが消費者に提供する特定の機能とバインドされる検証用公開鍵が必要である。特定の検証用公開鍵と特定のデジタルコンテンツあるいはその機能をバインドさせることで、特定のデジタルコンテンツやその機能の利用のみを許可する利用許可証を実現することができる。

## 【 0 0 5 3 】

利用許可証と検証用公開鍵に公開鍵暗号技術を利用しているのは、検証用公開鍵を公開可能とするためである。検証用公開鍵が公開鍵であれば、それを公開しても利用許可証の安全性を損なうことがない。このことは、検証用公開鍵の送受信や管理を楽にするだけでなく、利用許可証の正当性を第三者が検証できるようになり、後のトラブルを防ぐことが可能になるという利点がある。

## 【 0 0 5 4 】

検証用公開鍵はプロバイダからの依頼によって、センタ 1 0 2 で作成され、検証用公開鍵情報と呼ばれるデータに含まれて依頼者に送付される。センタ 1 0 2 は、検証用公開鍵の発行の要求を受け取ると新しい公開鍵ペアを作成し、その公開鍵と秘密鍵を、公開鍵ペアを一意に識別するための情報である検証用公開鍵識別子とともに保持した後、その公開鍵と検証用公開鍵識別子を含む検証用公開鍵情報を依頼者に送付する。検証用公開鍵情報を受け取ったプロバイダを、その検

証用公開鍵情報あるいは該検証用公開鍵情報に含まれる検証用公開鍵のユーザと呼ぶ。

## 【 0 0 5 5 】

特定の検証用公開鍵と特定のデジタルコンテンツあるいはその機能のバインドに関してセンタ 1 0 2 は関知しない。そのバインドを決定するのは、検証用公開鍵の発行を受けたプロバイダであり、該プロバイダは、自分が決定した、特定のデジタルコンテンツやその機能と検証用公開鍵とのバインドの情報を保持しておかなければならない。

## 【 0 0 5 6 】

利用許可証は、該許可証に対応する検証用公開鍵とバインドされた特定のデジタルコンテンツあるいはその機能の利用を許可するデータである。消費者がデジタルコンテンツを利用するコンピュータシステムに保持され、デジタルコンテンツの利用時にその正当性が検証される。

## 【 0 0 5 7 】

利用許可証がデジタルデータであるので、利用と許可された以外の利用者が利用許可証のコピーを使って、デジタルコンテンツを利用する危険がある。これを防止するために、利用許可証は消費者秘密情報とよばれる情報無しには、その正当性を検証できないように構成されている。消費者秘密情報は、利用許可証が正当であると認められる範囲を限定するための情報であり、ある消費者秘密情報にあわせて作成された利用許可証は、別の消費者秘密情報と共に利用しても正当なものと認められることはない。

## 【 0 0 5 8 】

たとえば、消費者秘密情報がコンピュータシステムに記憶されているコンピュータシステム毎に異なる数値として実現されれば、特定のコンピュータでのみ有効な利用許可証を実現することができる。この場合、消費者は、自分がそこでデジタルコンテンツを使うであろうコンピュータシステムが持つ消費者秘密情報にあわせた利用許可証を取得する。以降、該消費者は、該コンピュータシステムの上でのみデジタルコンテンツの利用が可能になるが、同じ利用証明証を使って他のコンピュータシステム上でデジタルコンテンツを利用することはできない。

## 【0059】

デジタルコンテンツの使用が特定のコンピュータシステムに限定されるのが不便な場合は、ICカード等の携帯型記憶装置を利用する。この場合、消費者秘密情報は、携帯型記憶装置に記憶されている携帯型記憶装置毎に異なるように実現される。この場合、消費者は、自分が所持する携帯型記憶装置に含まれる消費者秘密情報にあわせた利用許可証を取得する。以降、消費者は、自己が所持している携帯型記憶装置と取得した利用許可証を共に使用する場合に限りデジタルコンテンツを利用することができるが、携帯型記憶装置がなしにはデジタルコンテンツを利用することはできない。リムーバブルディスクやMO等の記憶メディアを携帯型記憶装置として利用してもよい。

## 【0060】

消費者秘密情報は、消費者すらその値を参照することができないように記憶されたデータとして実現される。また、コンピュータシステムや携帯型記憶装置の各種特徴量をもとに値を計算するアルゴリズムのみが記憶されており、消費者秘密情報が参照されるたびにそのアルゴリズムによる計算がおこなわれ、その結果が消費者秘密情報として使用されるのでもよい。その他にも実現方法はいくつかあるが、いかなる方法であっても消費者秘密情報の内容を知っているのは利用許可証の発行者である利用許可証発行センタのみである。

## 【0061】

各消費者秘密情報には、消費者識別子と呼ばれる識別子が割り当てられている。各消費者秘密情報がセンタ以外のエンティティにとって秘密のデータであるのと異なり、消費者識別子は誰でも参照できるデータである。消費者識別子は、消費者が利用許可証を依頼する際に、どの消費者秘密情報にあわせた利用許可証を要求しているのかを特定するために使用される。

## 【0062】

特に本実施例では、消費者識別子は個々の消費者を特定するのに使用される。同じ消費者が使っている複数のコンピュータであっても、それぞれが保持している消費者秘密情報が異なれば、別々の消費者識別子が割り当てられており、別々の消費者であると認識される。

## 【 0 0 6 3 】

検証用公開鍵情報のデータ構造は以下のようである。

## 【 0 0 6 4 】

## 【表 1】

検証用公開鍵情報：：＝ {

発行者フィールド，  
受領者フィールド，  
発行日フィールド，  
有効期間開始日時フィールド，  
有効期間終了日時フィールド，  
検証用公開鍵識別子フィールド，  
公開鍵情報フィールド，  
デジタル署名フィールド  
}

## 【 0 0 6 5 】

発行者フィールド：この検証用公開鍵情報の発行者であるセンタの識別子が記載される。

受領者フィールド：この検証用公開鍵情報の受領者であるプロバイダの識別子が記載される。

発行日フィールド：この検証用公開鍵情報の発行日が記載される。

有効期間開始日時フィールド：この検証用公開鍵情報の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この検証用公開鍵情報の有効期間の終了日時が記載される。

検証用公開鍵識別子フィールド：センタがこの検証用公開鍵に割り当てた検証用公開鍵識別子が記載される。

公開鍵情報：利用許可証を検証する際に使用する検証用公開鍵の情報が記載される。使用する公開鍵暗号アルゴリズムの指定と、公開鍵の値を含む。

デジタル署名フィールド：発行者であるセンタによるこの検証用公開鍵情報全体

に対するデジタル署名が記載される。

【 0 0 6 6 】

利用許可証のデータ構造は以下のようである。

【 0 0 6 7 】

【表 2】

利用許可証：：＝ {

発行者フィールド，  
受領者フィールド，  
発行日フィールド，  
利用許可証識別子フィールド，  
公開鍵識別子フィールド，  
利用条件フィールド，  
証明値フィールド，  
デジタル署名フィールド  
}

【 0 0 6 8 】

発行者フィールド：この利用許可証の発行者であるセンタの識別子が記載される。

受領者フィールド：この利用許可証の受領者である消費者の識別子が記載される。

発行日フィールド：この利用許可証の発行日が記載される。

利用許可証識別子フィールド：センタがこの利用許可証に割り当てた識別子が記載される。

公開鍵識別子フィールド：この利用許可証に対応する検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

利用条件フィールド：デジタルコンテンツの範囲を限定する条件である利用条件が記載される。

証明値フィールド：この利用許可証の公開鍵識別子フィールドに記載された識別子が割り当てられた検証用公開鍵に対応する秘密鍵をもとに作成された証明値が

記載される。

デジタル署名フィールド：発行者であるセンタによるこの利用許可証全体に対するデジタル署名が記載される。

【 0 0 6 9 】

利用条件フィールドに記載される。利用条件には、この利用許可証で有効となるデジタルコンテンツ利用の範囲を限定するための条件が記載される。

【 0 0 7 0 】

利用条件のデータ構造を以下に示す。

【 0 0 7 1 】

【表 3】

利用条件：：＝ {  
     有効期間開始日時フィールド，  
     有効期間終了日時フィールド，  
     . . .  
 }

【 0 0 7 2 】

有効期間開始日時フィールド：この利用許可証の有効期間の開始日時が記載される。この日時以前には、デジタルコンテンツの利用はできない。

有効期間終了日時フィールド：この利用許可証の有効期間の終了日時が記載される。この日時以降には、デジタルコンテンツの利用はできない。

【 0 0 7 3 】

利用条件に指定された各種条件は、利用許可証の検証時に該条件が満足されているかどうかを検査される。利用条件に指定された各種条件が満足されていなければ、利用許可証の正当性の検証に失敗する。

【 0 0 7 4 】

利用条件には、有効期間の開始日時または終了日時以外にも、利用許可証の用途に応じて種々のものが記載される。

【 0 0 7 5 】

例えば、デジタルコンテンツの利用回数が特定の回数以下に限定される場合に

は、その限定回数を利用条件に記載しておき、利用許可証の検査の際に該限定回数を超えていないかどうかを確認すればよい。

【0076】

また、デジタルコンテンツの利用時にいくらかの料金を徴収する場合には、その金額を利用条件に記載しておき、利用許可証の検査の際に該料金をプリペイドの度数から引き落とす等の処理を実行すればよい。

【0077】

あるいは、デジタルコンテンツが持つ機能のうちの特定の機能の利用のみを許す場合には、その機能を特定する情報を利用条件に記載しておき、利用許可証の検査の際にユーザが利用しようとする機能が利用条件に記載されたものであるかどうかを確認すればよい。

【0078】

〔証明値〕

証明値は利用許可証に含まれるデータで、センタが作成した検証用公開鍵に対応する秘密鍵を元に作成されたデータであり、利用許可証が特定の検証用公開鍵とのみ対応する事を保証するためのものである。また、証明値の作成には、消費者秘密情報も使用され、特定のコンピュータシステム上での使用のみ許したり、あるいは、特定の携帯型記憶装置と組み合わせた場合にのみ使用を許したりといった制御も可能である。さらに、証明値の作成には、利用許可証に記載された利用条件も使用され、特定の利用条件を満足する場合にのみ利用可能である事も保証される。

【0079】

証明値  $t$  は法数  $n$ 、検証用公開鍵  $e$ 、秘密鍵  $d$ 、消費者秘密情報  $u$ 、利用条件  $l$  から以下の式にしたがって作成される。

【0080】

〔数1〕

$$t = d - f(n, e, u, l) \quad (1)$$

ここで、関数  $f()$  は公開された一方向性関数である。たとえば、SHA-1 あるいは MD5 等の暗号学的一方向性ハッシュ関数を使用される。



## 【0081】

式(1)でわかるように、証明値 $t$ は、法数 $n$ 、検証用公開鍵 $e$ 、消費者秘密情報 $u$ 、利用条件 $l$ とともに使用した場合にのみ秘密鍵 $d$ と同じ働きをする。どれ一つを差し替えても秘密鍵 $d$ と同じ働きをすることはない。

## 【0082】

## [利用許可証の検証とデジタルコンテンツの利用]

本実施例では、消費者がデジタルコンテンツを利用する際に、必要に応じて該デジタルコンテンツ全体、あるいはその一部の機能に対する利用許可証の正当性を検証し、デジタルコンテンツ全体あるいはその一部の機能の使用の利用を消費者が許可されているかどうかを検査し、許可されている場合にのみ利用を許す。

## 【0083】

図35は、本発明を適用したデジタルコンテンツであるアプリケーションソフトウェアの構成を示した図である。本ソフトウェアは、利用者からの命令により2つの機能を実行するが、どの機能も実行されるまえに、利用者が利用許可証を持っているかどうかを確認され、利用者が正しい利用許可証を所持する場合にのみ機能が実行される。それぞれの機能には異なる検証用公開鍵が割り当てられているので、それぞれ異なる利用証明証が必要である。

## 【0084】

また、本ソフトウェアでは、消費者が消費者識別子と消費者秘密情報を含む携帯型記憶装置を所持しており、該消費者がデジタルコンテンツを使用するための利用許可証も該携帯型記憶装置に記憶されている。

## 【0085】

本ソフトウェア3501は、入出力制御部3502、処理制御部3503、第1の機能の実行部3504、第2の機能の実行部3505、第1の利用許可証検査部3506、第2の利用許可証検査部3507、携帯型記憶装置制御部3508からなり、携帯型記憶装置制御部3508をとおして携帯型記憶装置3511と接続している。

## 【0086】

それぞれの構成要素の役割を以下に示す。

## 【 0 0 8 7 】

入出力制御部 3 5 0 2 : 利用者からの入力あるいは、利用者への出力を制御する。

処理制御部 3 5 0 3 : 入出力制御部 3 5 0 2 からの利用者の命令を受け取り、命令に応じて第 1 の機能の実行部 3 5 0 4 、第 2 の機能の実行部 3 5 0 5 を呼び出し、機能の実行の結果を受け取って、入出力制御部 3 5 0 2 を介して利用者に出力する。

第 1 の機能の実行部 3 5 0 4 : 処理制御部 3 5 0 3 からの呼び出しに応じて、第 1 の機能を実行し、結果を処理制御部 3 5 0 3 に返す。実行の前に第 1 の利用許可証検査部 3 5 0 6 を呼び出し、利用者が第 1 の機能に対応する正しい利用許可証を所持している事を確認する。

第 2 の機能の実行部 3 5 0 5 : 処理制御部 3 5 0 3 からの呼び出しに応じて、第 2 の機能を実行し、結果を処理制御部 3 5 0 3 に返す。実行の前に第 2 の利用許可証検査部 3 5 0 7 を呼び出し、利用者が第 2 の機能に対応する正しい利用許可証を所持している事を確認する。

第 1 の利用許可証検査部 3 5 0 6 : 第 1 の機能の実行部 3 5 0 4 からの呼び出しに応じて、利用者が第 1 の機能に対応する正しい利用許可証を所持しているかどうかを検査し、結果を第 1 の機能の実行部 3 5 0 4 に返す。利用許可証の検査のために、携帯型記憶装置制御部 3 5 0 8 を介して、携帯型記憶装置 3 5 1 1 とデータの交換を行う。

第 2 の利用許可証検査部 3 5 0 7 : 第 2 の機能の実行部 3 5 0 5 からの呼び出しに応じて、利用者が第 2 の機能に対応する正しい利用許可証を所持しているかどうかを検査し、結果を第 2 の機能の実行部 3 5 0 5 に返す。利用許可証の検査のために、携帯型記憶装置制御部 3 5 0 8 を介して、携帯型記憶装置 3 5 1 1 とデータの交換を行う。

携帯型記憶装置制御部 3 5 0 8 : 携帯型記憶装置 3 5 1 1 とのデータ交換を制御する。

## 【 0 0 8 8 】

図 2 8 は、図 3 5 に示したソフトウェアの第 1 の利用許可証検査部 3 5 0 6 と

、該ソフトウェアに接続している携帯型記憶装置 3 5 1 1 の内部構成を示したものである。第 1 の利用許可証検証部 3 5 0 6 は、チャレンジと呼ぶ乱数値を携帯型記憶装置 3 5 1 1 に送付し、携帯型記憶装置 3 5 1 1 は受け取ったチャレンジと保持している利用許可証からレスポンスと呼ぶ値を計算して出力し、利用許可証検査部 3 5 0 6 がレスポンスの正しさを検査する事で、携帯型記憶装置 3 5 1 1 に保持されている利用許可証の正当性を検証する。

## 【 0 0 8 9 】

第 1 の利用許可証検査部 3 5 0 6 は、条件判定対象情報生成部 2 8 0 1、チャレンジ生成部 2 8 0 2、公開鍵情報記憶部 2 8 0 3、レスポンス検査部 2 8 0 4 から構成される。

## 【 0 0 9 0 】

利用許可証検査部 3 5 0 6 の各部の役割を以下に示す。

## 【 0 0 9 1 】

条件判定対象情報生成部 2 8 0 1：利用許可証に記載されている利用条件が特定の条件を満たす場合にのみ第 1 の機能を実行する場合、その判断の対象となる情報を生成する。

チャレンジ生成部 2 8 0 2：携帯型記憶装置 3 5 1 1 に送付するチャレンジを生成する。

公開鍵情報記憶部 2 8 0 3：第 1 の機能に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

レスポンス検査部 2 8 0 4：携帯型記憶装置 3 5 1 1 が作成したレスポンスの正しさを検査する。

## 【 0 0 9 2 】

また、携帯型記憶装置 3 5 1 1 は入出力制御部 2 8 1 1、消費者秘密情報記憶部 2 8 1 2、レスポンス計算部 2 8 1 3、利用条件判定部 2 8 1 4、利用許可証記憶部 2 8 1 5 から構成される。

## 【 0 0 9 3 】

携帯型記憶装置 3 5 1 1 の各部の役割を以下に示す。

## 【 0 0 9 4 】

入出力制御部 2 8 1 1 : ソフトウェア 3 5 0 1 との間のデータの入出力を制御する。

消費者秘密情報記憶部 2 8 1 2 : 消費者秘密情報を保持する。

レスポンス計算部 2 8 1 3 : 第 1 の利用許可証検査部 3 5 0 6 に送付するレスポンスを計算する。

利用条件判定部 2 8 1 4 : 利用許可証に記載されている利用条件が満たされているかどうかを判定する。

利用許可証記憶部 2 8 1 5 : 利用許可証が複数保持される。

#### 【 0 0 9 5 】

図 2 9 は、第 1 の機能に対する利用許可証の検査の際の第 1 の利用許可証検証部 3 5 0 6 と携帯型記憶装置 3 5 1 1 の動作を示すフローチャートである。図 2 9 に従って利用許可証の検査の際の利用許可証検査部 3 5 0 6 と携帯型記憶装置 3 5 1 1 の動作を説明する。

#### 【 0 0 9 6 】

利用許可証の検査の動作は第 1 の利用許可証検証部 3 5 0 6 から始まる。

#### 【 0 0 9 7 】

まず、チャレンジ生成部 2 8 0 2 でチャレンジ C が作成される ( 2 9 0 1 ) 。チャレンジは検査を行うたびに異なる乱数値であり、チャレンジ生成部 2 8 0 2 は乱数生成機能を内包している。

#### 【 0 0 9 8 】

チャレンジが生成された後、生成されたチャレンジ C、公開鍵情報記憶部 2 8 0 3 に保持されている検証用公開鍵の識別子 ID と法数 n および公開鍵 e、条件判定対象情報生成部 2 8 0 1 で生成された条件判定対象情報 s が、携帯型記憶装置制御部 3 5 0 8 を介して携帯型記憶装置 3 5 1 1 に送付される ( 2 9 0 2 ) 。

#### 【 0 0 9 9 】

C、ID、n、e、s を受け取った携帯型記憶装置 3 5 1 1 は、まず利用許可証記憶部 2 8 1 5 に保持されている利用許可証のうち検証用公開鍵識別子 ID に対応するものを選択する ( 2 9 0 3 ) 。この選択は、利用許可証記憶部 2 8 1 5 に保持されている利用許可証のうち、その公開鍵識別子フィールドの値が ID と

等しいかどうかを調べる事で行われる。ここで該当する利用許可証が見つからなければ、エラーが入出力制御部 2811 を介して第 1 の利用許可証検査部 3506 に送付され (2908)、終了する。

#### 【0100】

該当する利用許可証が見つかった場合には、利用条件判定部 2814 で該利用許可証に含まれる利用条件 1 が満たされているかどうか判定される (2904)。利用条件 1 に記載されている利用許可証の有効期間開始や終了のチェックのために、利用条件判定部 2814 は時計を内蔵している。また、第 1 の利用許可証検査部 3506 から条件指定  $s$  が入力されている場合、条件判定対象情報  $s$  が利用条件 1 を満たすかどうかもここで判定される。

#### 【0101】

2904 で、利用条件 1 が満たされていないと判断された場合、エラーが入出力制御部 2811 を介して第 1 の利用許可証検査部 3506 に送付され (2908)、終了する。

#### 【0102】

2904 で、利用条件 1 が満たされていると判断された場合、レスポンス計算部 2813 でレスポンス  $R$  が計算され (2905)、入出力制御部 2811 を介して第 1 の利用許可証検査部 3506 に送付される (2906)。レスポンス  $R$  は、入出力制御部 2811 を介して第 1 の利用許可証検査部 3506 から入力されたチャレンジ  $C$ 、法数  $n$ 、公開鍵  $e$ 、2903 で選択された利用許可証に含まれる証明値  $t$  と利用条件 1、消費者秘密情報記憶部 2812 に保持されている消費者秘密情報  $u$  から、以下の (2) 式にしたがって計算される。

#### 【0103】

【数 2】

$$R = C^{t+f(n,e,u,l)} \bmod n \quad (2)$$

携帯型記憶装置制御部 3508 を介してレスポンス  $R$  を受け取った第 1 の利用許可証検査部 3506 は、レスポンス検査部 2804 でレスポンス  $R$  の正当性を検査する (2907)。検査にはレスポンス  $R$  の他に、チャレンジ生成部 2802 が生成したチャレンジ  $C$ 、公開鍵情報記憶部 2803 が記憶している法数  $n$ 、

公開鍵  $e$  が使用される。(3) の式が成り立てば検証成功、そうでなければ失敗である。

【0104】

【数3】

$$C \equiv R^e \pmod{n} \quad (3)$$

(1) (2) (3) の式からわかるように、利用許可証の検査は、基本的には証明値  $t$  が秘密鍵  $d$  と同じ働きができるかどうかを判定する処理であり、法数や公開鍵、証明値、利用条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なるデジタルコンテンツの利用許可証を流用したり、他人の利用許可証を利用したり、利用条件を改竄したりといった攻撃は困難である。

【0105】

前述したように、利用条件 1 には、利用許可証の有効期間以外に多くの条件が記載可能である。それらの条件のうち、条件判定の対象となる情報が携帯型記憶装置内にない場合は、その情報は携帯型記憶装置 3511 の外部から条件判定対象情報  $s$  として供給される。たとえば、図 35 に示したソフトウェアの第 2 の機能が実行された場合にのみ利用可能であると利用条件 1 に記載されている場合には、第 2 の機能が実行されたかどうかを示す情報が条件判定対象情報生成部 2801 で生成され、条件判定対象情報  $s$  として携帯型記憶装置 3511 の外から供給される。

【0106】

図 35 に示したソフトウェアの第 2 の利用許可証検査部 3507 も図 28 に示した第 1 の利用許可証検査部 3506 と同様の内部構成を持ち、図 29 と同様の動作を行う。

【0107】

図 36 は、本発明を適用したデジタルコンテンツプロセッシングソフトウェアである。本ソフトウェアは、文書・画像・音楽・映像といったデジタルコンテンツに対して表示・編集・印刷が可能なソフトウェアである。本ソフトウェアでは、コンテンツに対して操作を行う前に、利用者が正しい利用許可証を持っている

かどうかを確認され、利用者が正しい利用許可証を所持する場合にのみ操作が可能である。

【0108】

ソフトウェア3601は、入出力制御部3602、処理制御部3603、表示実行部3604、編集実行部3605、印刷実行部3606、コンテンツデータ記憶部3607、利用許可証検査部3608からなる。

【0109】

それぞれの構成要素の役割を以下に示す。

【0110】

入出力制御部3602：利用者からの入力あるいは、利用者への出力を制御する。

処理制御部3603：入出力制御部3602からの利用者の命令を受け取り、命令に応じてデジタルコンテンツの表示、編集、印刷といった機能を実行する。

表示実行部3604：入出力制御部3602からの呼び出しに応じてデジタルコンテンツの表示を実行する。実行の前に利用許可証検査部3608を呼び出し、利用者が現在操作中のデジタルコンテンツの表示に対する正しい利用許可証を所持している事を確認する。

編集実行部3605：入出力制御部3602からの呼び出しに応じてデジタルコンテンツの編集を実行する。実行の前に利用許可証検査部3608を呼び出し、利用者が現在操作中のデジタルコンテンツの編集に対する正しい利用許可証を所持している事を確認する。

印刷実行部3606：入出力制御部3602からの呼び出しに応じてデジタルコンテンツの印刷を実行する。実行の前に利用許可証検査部3608を呼び出し、利用者が現在操作中のデジタルコンテンツの印刷に対する正しい利用許可証を所持している事を確認する。

コンテンツデータ記憶部3607：利用者が現在操作中のデジタルコンテンツのデータを保持する。

利用許可証検査部3608：表示実行部3604、編集実行部3605、印刷実行部3606から呼び出され、利用者が、現在操作中のデジタルコンテンツに対

して指定された操作を実行可能な利用許可証を所持しているかどうかを検査する。

#### 【0111】

また、本ソフトウェアが動作するコンピュータ上には、消費者秘密情報や利用許可証を保持し、利用許可証の正当性の検査に使用する情報を作成して、利用許可証検査部3608に送付する利用許可証明部3611が存在する。

#### 【0112】

図37に本ソフトウェアが操作するデジタルコンテンツのデータ構造を示す。

#### 【0113】

本ソフトウェアが操作するデジタルコンテンツは、複数のページからなる。各ページに施される操作の種類毎に検証用公開鍵が割り当てられており、各ページの各機能毎に、必要となる利用許可証が異なる。

#### 【0114】

デジタルコンテンツ3701は、3702、3703、3704といったページ毎のデータに別れている。各ページデータ3711は、そのページの表示に割り当てられた検証用公開鍵の情報3712、同じページの編集に割り当てられた検証用公開鍵の情報3713、同じページの印刷用に割り当てられた検証用公開鍵の情報3714、および、そのページのデータ本体3715からなる。さらに各検証用公開鍵の情報3721は、その検証用公開鍵に割り当てられた識別子3722、該検証用公開鍵の法数3723、該検証用公開鍵の公開鍵3724からなる。

#### 【0115】

たとえば、あるページの編集を行いたい場合に、該ページの編集用に割り当てられた検証用公開鍵に対応する利用証明証を消費者が所持しているかどうかを検査される。

#### 【0116】

デジタルコンテンツの改竄を防ぐために、本ソフトウェアが操作するデジタルコンテンツにはデジタル署名が施される。デジタル署名3705はデジタルコンテンツ3701の最後尾に付属しており、該コンテンツが改竄されていないかど



うかを必要に応じて検査することができる。

【0117】

図30は、図36に示したソフトウェア3601の利用許可証検査部3608と、該ソフトウェアに対して利用許可証の正当性の検査に使用する情報を供給する利用許可証明書部3611の内部構成を示したものである。利用許可証検査部3608は、チャレンジと呼ぶ乱数値を利用許可証明書部3611に送付し、利用許可証明書部3611は、受け取ったチャレンジからレスポンスと呼ぶ値を計算して出力し、利用許可証検査部3608がレスポンスの正しさを検査する事で、利用許可証明書部3611に保持されている利用許可証の正当性を検証する。

【0118】

利用許可証検査部3608は、入出力インタフェース3001、チャレンジ生成部3002、条件判定対象情報生成部3003、公開鍵情報記憶部3004、レスポンス検査部3005、利用条件判定部3006、利用許可証記憶部3007、通信制御部3008から構成される。

【0119】

利用許可証検査部3608の各部の役割を以下に示す。

【0120】

入出力インタフェース3001：表示実行部3604、編集実行部3605、印刷実行部3606からの入力をうけ、利用許可証の検査結果を出力するインタフェース。

チャレンジ生成部3002：利用許可証明書部3611に送付するチャレンジを生成する。

条件判定対象情報生成部3003：利用許可証に記載されている利用条件が特定の条件を満たす場合にのみ機能を実行する場合、その判断の対象となる情報を生成する。

公開鍵情報記憶部3004：利用許可証の検査に使用する検証用公開鍵に関する情報を記憶する。

レスポンス検査部3005：利用許可証明書部3611が作成したレスポンスの正しさを検査する。

利用条件判定部 3 0 0 6 : 利用許可証に記載されている利用条件が満たされているかどうかを判定する。

利用許可証記憶部 3 0 0 7 : 利用許可証明部 3 6 1 1 から取り出した利用許可証を保持する。

通信制御部 3 0 0 8 : 利用許可証明部 3 6 1 1 との間の通信を制御する。

#### 【 0 1 2 1 】

また、利用許可証明部 3 6 1 1 は、入出力制御部 3 0 1 1、消費者秘密情報記憶部 3 0 1 2、レスポンス計算部 3 0 1 3、利用許可証記憶部 3 0 1 4 から構成される。

#### 【 0 1 2 2 】

利用許可証明部 3 6 1 1 の各部の役割を以下に示す。

#### 【 0 1 2 3 】

入出力制御部 3 0 1 1 : 利用許可証検査部 3 6 0 8 との間の通信を制御する。

消費者秘密情報記憶部 3 0 1 2 : 消費者秘密情報を保持する。

レスポンス計算部 3 0 1 3 : 利用許可証検査部 3 6 0 8 に送付するレスポンスを計算する。

利用許可証記憶部 3 0 1 4 : 利用許可証が複数保持される。

#### 【 0 1 2 4 】

図 3 1 は、利用許可証の検証の際の利用許可証検査部 3 6 0 8 と利用許可証明部 3 6 1 1 の動作を示すフローチャートである。図 3 1 に従って利用許可証の検証の際の利用許可証検査部 3 6 0 8 と利用許可証明部 3 6 1 1 の動作を説明する。

#### 【 0 1 2 5 】

図 3 7 に示したデジタルコンテンツのあるページに対して表示・編集・印刷がソフトウェアの利用者から指示された場合、表示実行部 3 6 0 4、編集実行部 3 6 0 5 あるいは印刷実行部 3 6 0 6 は、利用許可証検査部 3 6 0 8 を呼び出して利用許可証の検査を行う。その際、表示実行部 3 6 0 4、編集実行部 3 6 0 5 あるいは印刷実行部 3 6 0 6 は、現在対象となっているページの、実行しようとする機能に割り当てられた検証用公開鍵の情報（検証用公開鍵識別子 ID、法数 n

、公開鍵e)をコンテンツデータ記憶部3607に記憶されているデジタルコンテンツから取り出して、入出力インタフェース3001を介して利用許可証検査部3608に入力する。利用許可証検査部3608は、この入力を受けた時点から利用許可証の検査を開始する。

#### 【0126】

利用許可証検査部3608は、まず最初に、入出力インタフェース3001を介して入力された検証用公開鍵の情報を公開鍵情報記憶部3004に記憶する(3100)。

#### 【0127】

次に、利用許可証検査部3608は、通信制御部3008を介して利用許可証明書部3611の利用許可証記憶部3014にアクセスし、利用許可証記憶部3014に保持されている利用許可証のうち、利用許可証の検査に使用可能なものを探す(3101)。利用許可証記憶部3014に保持されている利用許可証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部3004に保持されている検証用公開鍵識別子と一致するものが、求める利用許可証である。ここで該当する利用許可証が見つからなければ、利用許可証の検査は失敗であり、エラー処理の後(3109)、終了する。

#### 【0128】

該当する利用許可証が見つかった場合には、該利用許可証が取り出され、利用許可証検査部3608の利用許可証記憶部3007に記憶される(3102)。

#### 【0129】

次に、利用条件判定部3006で、利用許可証記憶部3007に保持されている利用許可証に含まれる利用条件1が満たされているかどうか判定される(3103)。利用条件1に記載されている利用許可証の有効期間開始や終了のチェックのために、利用条件判定部3006は時計を内蔵している。また、条件判定対象情報生成部3003で生成された条件判定対象情報sが存在する場合、条件判定対象情報sが利用条件1を満たすかどうかでもここで判定される。

#### 【0130】

3103で、利用条件1が満たされていないと判断された場合、利用許可証の

検査は失敗であり、エラー処理の後（3109）、終了する。

【0131】

3103で、利用条件1が満たされていると判断された場合、チャレンジ生成部3002でチャレンジCが作成される（3104）。チャレンジは検証を行うたびに異なる乱数値であり、チャレンジ生成部3002は乱数生成機能を内包している。

【0132】

チャレンジが生成された後、生成されたチャレンジC、公開鍵情報記憶部3004に保持されている法数nおよび公開鍵e、利用許可証記憶部3007に記憶されている利用許可証が含む利用条件1が、通信制御部3008を介して利用許可証明部3611に送付される（3105）。

【0133】

チャレンジを受け取った利用許可証明部3611は、レスポンス計算部3013でレスポンスRを計算し（3106）、通信制御部3011を介して利用許可証検査部3608に送付される（3107）。レスポンスRは、通信制御部3011を介して利用許可証検査部3608から入力されたチャレンジC、法数n、公開鍵e、利用条件1、消費者秘密情報記憶部3013に保持されている消費者秘密情報uから、以下の（4）式にしたがって計算される。

【0134】

【数4】

$$R = C^{f(n,e,u,l)} \bmod n \quad (4)$$

通信制御部3008を介してレスポンスRを受け取った利用許可証検査部3608は、レスポンス検査部3005でレスポンスRの正当性を検査する（3108）。検証にはレスポンスRの他に、チャレンジ生成部3002が生成したチャレンジC、公開鍵情報記憶部3004が記憶している法数n、公開鍵e、利用許可証記憶部3007が保持している利用許可証に含まれる証明値tが使用される。（5）の式が成り立てば検証成功、そうでなければ失敗である。

【0135】

【数5】

$$C \equiv (C^t R)^e \pmod{n} \quad (5)$$

(1) (4) (5) の式からわかるように、法数や公開鍵、証明値、利用条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検査に成功する。検証用公開鍵が異なるデジタルコンテンツの利用許可証を流用したり、他人の利用許可証を利用したり、利用条件を改竄したりといった攻撃は困難である。

#### 【0136】

前述したように、利用条件 1 には、利用許可証の有効期間以外に多くの条件が記載可能である。たとえば、利用可能な回数を利用条件 1 に指定することは好適な例である。この場合、条件判定対象情報生成部 3 0 0 3 に現在までの使用回数を保持する機構を設けておき、3 1 0 3 の判断の際に条件判定対象情報 s として利用条件判定部 3 0 0 6 に送付し、そこで利用条件 1 に記載されている利用可能な回数と比較すればよい。

#### 【0137】

編集のように長時間かかる作業の際は、編集作業の開始時に利用許可証の検査に成功したとしても、編集作業の途中で利用許可証の有効期間が切れてしまうことがありえる。このような場合には、数分毎に、利用許可証の検査をおこない、利用許可証の有効期間が切れていることがわかった場合には、その時点で編集が実行できなくなるように構成すればよい。

#### 【0138】

デジタルコンテンツに含まれるデータ本体 3 7 1 5 が、特に暗号化等の施されていない形式であった場合、デジタルコンテンツのファイルからデータ本体のみを取り出すことで、利用許可証の検査なしに、デジタルコンテンツの内容にアクセスできる可能性がある。これを防ぐためには、データ本体 3 7 1 5 には暗号化されたデータを入れておけばよい。利用許可証の検査に成功した場合にのみ一時的に復号し、各種機能を実行するようにすることで、ファイルからデジタルコンテンツの内容が漏れることを防ぐことができる。

#### 【0139】

図 3 8 は、本発明を適用したデジタルコンテンツを復号するソフトウェアである。本ソフトウェアは、暗号化された状態で存在する文書・画像・音楽・映像と

いったデジタルコンテンツを復号して利用可能な形式として出力するものである、復デジタルコンテンツの復号には利用許可証が必要であり、本ソフトウェアは、復号を実行する前に、本ソフトウェアの利用者が正しい利用許可証を所持しているかどうかを検査する。

#### 【0140】

ソフトウェア3801は、入出力制御部3802、復号部3803、利用許可証検査部3804からなる。

#### 【0141】

それぞれの構成要素の役割を以下に示す。

#### 【0142】

入出力制御部3802：利用者からの入力あるいは、利用者への出力を制御する。

復号部3803：暗号化されているデジタルコンテンツを復号する。

利用許可証検査部3804：復号部3803から呼び出され、利用者が、現在操作中のデジタルコンテンツを復号可能な利用許可証を所持しているかどうかを検査する。

#### 【0143】

また、本ソフトウェアが動作するコンピュータ上には、消費者秘密情報や利用許可証を保持し、利用許可証の正当性の検査に必要な情報を利用許可証検査部3804に送付する利用許可証明書部3811が存在する。

#### 【0144】

図39に本ソフトウェアが復号するデジタルコンテンツのデータ構造を示す。

#### 【0145】

本ソフトウェアが復号するデジタルコンテンツ3901は、暗号化されたデータ本体3903と、本デジタルコンテンツの復号に割り当てられた検証用公開鍵の情報3902、さらには、データ本体3903と検証用公開鍵の情報3902に対するデジタル署名3904からなる。デジタル署名3904は、デジタルコンテンツの改竄を防ぐためのものである。デジタルコンテンツ3901の最後尾に付属しており、デジタルコンテンツ3901が改竄されていないかどうかを必

要に応じて検査することができる。

【0146】

図32は、図38に示したソフトウェア3801の利用許可証検査部3804と、該ソフトウェアに対して利用許可証の正当性の検査に使用する情報を供給する利用許可証明部3811の内部構成を示したものである。利用許可証検査部3608は、利用許可証明部3811が保持している利用許可証をとりだし、その正当性を検証する。

【0147】

利用許可証検査部3804は、入出力インタフェース3201、条件判定対象情報生成部3202、利用条件判定部3203、公開鍵情報記憶部3204、証明値検査部3205、利用許可証記憶部3206、通信制御部3207、消費者秘密情報記憶部3208から構成される。

【0148】

利用許可証検査部3804の各部の役割を以下に示す。

【0149】

入出力インタフェース3201：復号部3803からの入力をうけ、利用許可証の検査結果を出力するインタフェース。

条件判定対象情報生成部3202：利用許可証に記載されている利用条件が特定の条件を満たす場合にのみデジタルコンテンツを復号する場合、その判断の対象となる情報を生成する。

利用条件判定部3203：利用許可証に記載されている利用条件が満たされているかどうかを判定する。

公開鍵情報記憶部3204：利用許可証の検査に使用する検証用公開鍵に関する情報を記憶する。

証明値検査部3205：利用許可証に記載されている証明値の正当性を検査する。

利用許可証記憶部3206：利用許可証明部3811から取り出した利用許可証を保持する。

通信制御部3207：利用許可証明部3811との間の通信を制御する。

消費者秘密情報記憶部 3 2 0 8 : 利用許可証明部 3 8 1 1 から取り出した消費者秘密情報を保持する。

【 0 1 5 0 】

また、利用許可証明部 3 8 1 1 は、通信制御部 3 2 1 1、消費者秘密情報記憶部 3 2 1 2、利用許可証記憶部 3 2 1 3 から構成される。

【 0 1 5 1 】

利用許可証明部 3 8 1 1 の各部の役割を以下に示す。

【 0 1 5 2 】

通信制御部 3 2 1 1 : 利用許可証検査部 3 8 0 4 との間のデータの入出力を制御する。

消費者秘密情報記憶部 3 2 1 2 : 消費者秘密情報を保持する。

利用許可証記憶部 3 2 1 3 : 利用許可証が複数保持される。

【 0 1 5 3 】

図 3 3 は、利用許可証の検証の際の利用許可証検査部 3 8 0 4 と利用許可証明部 3 8 1 1 の動作を示すフローチャートである。図 3 3 に従って利用許可証の検査の際の利用許可証検査部 3 8 0 4 と利用許可証明部 3 8 1 1 の動作を説明する。

【 0 1 5 4 】

図 3 9 に示したデジタルコンテンツの復号が利用者から指示された場合、復号部 3 8 0 3 は、利用許可証検査部 3 8 0 4 を呼び出して利用許可証の検証を行う。その際復号部 3 8 0 3 は、該デジタルコンテンツに付随している検証用公開鍵の情報（検証用公開鍵識別子 ID、法数  $n$ 、公開鍵  $e$ ）を取り出して、入出力インターフェース 3 2 0 1 を介して利用許可証検査部 3 8 0 4 に入力する。利用許可証検査部 3 8 0 4 は、この入力を受けた時点から利用許可証の検査を開始する。

【 0 1 5 5 】

利用許可証検査部 3 8 0 4 は、まず、入出力インターフェース 3 2 0 1 を介して入力された検証用公開鍵の情報を公開鍵情報記憶部 3 2 0 4 に記憶する（3 3 0 0）。次に通信制御部 3 2 0 7 を介して利用許可証明部 3 8 1 1 の利用許可証記憶部 3 2 1 3 にアクセスし、利用許可証記憶部 3 2 1 3 に保持されている利用



許可証のうち、利用許可証検査部 3 8 0 4 による利用許可証の検査に使用可能なものを探す (3 3 0 1)。利用許可証記憶部 3 2 1 1 に保持されている利用許可証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部 3 2 0 4 に保持されている検証用公開鍵識別子と一致するものが、求める利用許可証である。ここで該当する利用許可証が見つからなければ、利用許可証の検査は失敗であり、エラー処理の後 (3 3 0 6)、終了する。

## 【0 1 5 6】

該当する利用許可証が見つかった場合には、該利用許可証が取り出され、利用許可証検査部 3 8 0 4 の利用許可証記憶部 3 2 0 6 に記憶される (3 3 0 2)。

## 【0 1 5 7】

次に、利用条件判定部 3 2 0 3 で、利用許可証記憶部 3 2 0 6 に保持されている利用許可証に含まれる利用条件 1 が満たされているかどうか判定される (3 3 0 3)。利用条件 1 に記載されている利用許可証の有効期間開始や終了のチェックのために、利用条件判定部 3 2 0 3 は時計を内蔵している。また、条件判定対象情報生成部 3 2 0 2 で生成された条件判定対象情報  $s$  が存在する場合、条件判定対象情報  $s$  が利用条件 1 を満たすかどうかもここで判定される。

## 【0 1 5 8】

3 3 0 3 で、利用条件 1 が満たされていないと判断された場合、利用許可証の検査は失敗であり、エラー処理の後 (3 3 0 6)、終了する。

## 【0 1 5 9】

3 3 0 3 で、利用条件 1 が満たされていると判断された場合、通信制御部 3 2 0 7 を介して利用許可証明部 3 8 1 1 の消費者秘密情報記憶部 3 2 1 2 にアクセスし、消費者秘密情報記憶部 3 2 1 2 に保持されている消費者秘密情報  $u$  を取り出し、利用許可証検査部 3 8 0 4 の消費者秘密情報記憶部 3 2 0 8 に記憶する (3 3 0 4)。

## 【0 1 6 0】

最後に、証明値検査部 3 2 0 5 で、利用許可証記憶部 3 2 0 6 に保持されている利用許可証に含まれる証明値  $t$  の正当性を検査する (3 3 0 5)。検証のために、証明値検査部 3 2 0 5 は乱数  $r$  を生成し、公開鍵情報記憶部 3 2 0 4 が記憶

している法数  $n$ 、公開鍵  $e$ 、利用許可証記憶部 3206 が保持している利用許可証に含まれる利用条件 1、消費者秘密情報記憶部 3208 が保持している消費者秘密情報  $u$  に対して (6) の式が成り立つかどうかを検査する。

【0161】

【数 6】

$$r \equiv (r^{t+f(n,e,u,l)})^e \bmod n \quad (6)$$

(1) (6) の式からわかるように、法数や公開鍵、証明値、利用条件、消費者秘密情報の組み合わせが正しい時のみ証明値の検査に成功する。検証用公開鍵が異なるデジタルコンテンツの利用許可証を流用したり、他人の利用許可証を利用したり、利用条件を改竄したりといった攻撃は困難である。

【0162】

圧縮されたデジタルコンテンツを伸長する際に、伸長のための利用許可証の検査をするよう構成する場合も、図 38 に示したソフトウェアと同様の構成と動作が利用できる。暗復号の処理が圧縮伸長の処理に変わるだけで、構成や動作はまったく同じものが利用できる。

【0163】

図 35 に示したソフトウェアや、図 37、図 39 に示したようなファイルといったデジタルコンテンツは、利用許可証を持たない消費者は使用できないので、消費者は、デジタルコンテンツ自体をいかなる流通経路を使って入手してもかまわない。したがって、デジタルコンテンツの提供者は、消費者にとって便利な様々な経路でデジタルコンテンツを配布することができる。たとえば、インターネット上の特定のサイトからのダウンロードでもよいし、CD-ROM 等に記憶させて配布するのもよい。衛星放送でデジタルコンテンツを放送してもよいし、デジタルコンテンツのコピーを友人同士で交換してもかまわない。

【0164】

〔検証用公開鍵情報の発行〕

検証用公開鍵情報はプロバイダからの依頼によって、センタで作成され、依頼したプロバイダに送付される。依頼の際には、検証用公開鍵情報依頼というデータが送受信される。通常、発信者は依頼をするプロバイダであり受信者は依頼を

受けるセンタであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに依頼を行ったりセンタの代わりに依頼を受けたりする場合には、プロバイダやセンタ以外のエンティティが発信者や受信者になってもよい。

## 【0165】

検証用公開鍵情報依頼のデータ構造を以下に示す。

## 【0166】

## 【表4】

検証用公開鍵情報依頼 ::= {  
     発信者フィールド,  
     受信者フィールド,  
     日時フィールド,  
     公開鍵仕様フィールド,  
     デジタル署名フィールド,  
     証明証フィールド  
 }

## 【0167】

発信者フィールド：この検証用公開鍵情報依頼の発信者の識別子が記載される。

発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報依頼の受信者の識別子が記載される。

受信者は通常センタであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報依頼の作成日時が記載される。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する依頼者の要望が記載される。検証用公開鍵を使用するプロバイダの識別子、公開鍵暗号アルゴリズム、鍵長の情報がここに記述できる。

デジタル署名フィールド：この検証用公開鍵情報依頼の発信者によるこの検証用公開鍵情報依頼に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報依頼のデジタル署名フィールドのデジ

タル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0168】

検証用公開鍵情報依頼を受け取ったセンタは、検証用公開鍵情報依頼に記載された公開鍵仕様にしたがって公開鍵ペアを作成し、検証用公開鍵情報を作成して依頼者に渡す。依頼された検証用公開鍵情報を作成するかしないか、あるいは、指定された公開鍵仕様通りに公開鍵を作成するかどうかはセンタが決定できる。

【0169】

検証用公開鍵情報を引き渡す際には、検証用公開鍵情報送付というデータが送受信される。通常、発信者は検証用公開鍵情報を作成したセンタであり、受信者は発行された検証用公開鍵情報を使用するプロバイダであるが、インターネットに接続されたその他のエンティティがセンタの代わりに検証用公開鍵情報の送付を行ったり、プロバイダの代わりに検証用公開鍵情報を受け取ったりする場合には、センタやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【0170】

検証用公開鍵情報送付のデータ構造を以下に示す。

【0171】

【表5】

検証用公開鍵情報送付 ::= {  
     発信者フィールド,  
     受信者フィールド,  
     日時フィールド,  
     検証用公開鍵情報フィールド,  
     デジタル署名フィールド,  
     証明証フィールド  
 }

【0172】

発信者フィールド：この検証用公開鍵情報送付の送付者の識別子が記載される。発信者は通常センタであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報送付の受信者の識別子が記載される。  
 受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報送付の作成日時が記載される。

検証用公開鍵情報フィールド：この検証用公開鍵情報送付で送られる検証用公開鍵情報が記載される。

デジタル署名フィールド：この検証用公開鍵情報送付の発信者によるこの検証用公開鍵情報送付に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報送付のデジタル署名フィールド、およびこの検証用公開鍵情報送付に含まれる検証用公開鍵情報のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

#### 【 0 1 7 3 】

##### 〔利用許可証仲介許諾〕

本実施例では、プロバイダとリテーラは独立に存立することが可能である。リテーラは多様なプロバイダが提供する多様なデジタルコンテンツの販売を行うことが可能であるし、特定のプロバイダが自己の提供するデジタルコンテンツを多くのリテーラに販売をしてもらうといったことも可能である。

#### 【 0 1 7 4 】

プロバイダにとっては、多くのリテーラに自己のデジタルコンテンツを販売してもらうことは基本的には有利であるが、信用度の低いリテーラに販売をされるのは、後のトラブルを招く可能性が高く許容できない。したがって、プロバイダは自己のデジタルコンテンツを取り扱えるリテーラをコントロールする必要がある。

#### 【 0 1 7 5 】

このコントロール可能にするために、本実施例では利用許可証仲介許諾というデータを使用する。

#### 【 0 1 7 6 】

利用許可証仲介許諾はプロバイダが特定のリテーラに対して自己の特定のデジ

タルコンテンツの販売を委託している事を証するデジタルデータであり、リテーラからの依頼を受けて作成され、依頼者に送付される。

【0177】

以降、単に仲介許諾といえは利用許可証仲介許諾を、仲介許諾証といえは利用許可証仲介許諾証を指すものとする。

【0178】

仲介許諾証のデータ構造を以下に示す。

【0179】

【表6】

仲介許諾証：：＝ {

発行者フィールド，  
受領者フィールド，  
発行日フィールド，  
仲介許諾識別子フィールド，  
有効期間開始日時フィールド，  
有効期間終了日時フィールド，  
公開鍵識別子フィールド，  
利用条件限定情報フィールド，  
デジタル署名フィールド

}

【0180】

発行者フィールド：この仲介許諾証の発行者であるプロバイダの識別子が記載される。

受領者フィールド：この仲介許諾証の受領者であるリテーラの識別子が記載される。

発行日フィールド：この仲介許諾証の発行日が記載される。

仲介許諾識別子フィールド：この仲介許諾証にプロバイダが割り当てた識別子が記載される。

有効期間開始日時フィールド：この仲介許諾証の有効期間の開始日時が記載され

る。

有効期間終了日時フィールド：この仲介許諾証の有効期間の終了日時が記載される。

公開鍵識別子フィールド：この仲介許諾証によって利用許可証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

利用条件限定情報フィールド：利用許可証に記載される利用条件の範囲を限定する情報である利用条件限定情報が記載される。

デジタル署名フィールド：発行者であるプロバイダによるこの仲介許諾証全体に対するデジタル署名が記載される。

#### 【0181】

利用条件限定情報フィールドに記載される利用条件限定情報によって、プロバイダはリテーラの仲介によって発行される利用許可証に記載される利用条件を詳細にコントロールすることができる。

#### 【0182】

利用条件限定情報のデータ構造を以下に示す。

#### 【0183】

#### 【表7】

利用条件限定情報：：＝ {  
     最短有効期間フィールド，  
     最長有効期間フィールド，  
     ...  
 }

#### 【0184】

最短有効期間フィールド：この仲介許諾証の受領者であるリテーラが仲介して発行される、この仲介許諾証の公開鍵識別子フィールドに指定された検証用公開鍵に対応する利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最低限度が記載される。該利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以上でなければならない。

最長有効期間フィールド：この仲介許諾証の受領者であるリテーラが仲介して発行される、この仲介証の公開鍵識別子フィールドに指定された検証用公開鍵に対応する利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最長限度が記載される。該利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以下でなければならない。

【0185】

利用条件限定情報には、最短有効期間あるいは最長有効期間以外にも、この仲介許諾証の公開鍵識別子フィールドで指定された検証用公開鍵とバインドされているデジタルコンテンツに応じて種々の限定を設定する事が可能である。

【0186】

例えば、デジタルコンテンツの利用回数が特定の回数以下に限定されるような場合、最小利用可能回数や最大利用可能回数を利用条件限定情報に記載しておき、その範囲内で利用条件に利用可能回数を指定するように構成する。

【0187】

また、デジタルコンテンツの利用時にいくらかの料金を課金あるいは徴収するために利用条件にその金額を指定する場合には、指定可能な金額の範囲を利用条件限定情報に記載する。

【0188】

さらに、デジタルコンテンツが持つ機能のうちの特定の機能の利用のみを許すために利用条件にその機能を指定する場合には、指定可能な機能の範囲を利用条件限定情報に記載する。

【0189】

[仲介許諾証の発行]

仲介許諾証はリテーラからの依頼によって、プロバイダで作成され、依頼したリテーラに送付される。依頼の際には、仲介許諾証依頼というデータが送受信される。通常、発信者は依頼をするリテーラであり受信者は依頼を受けるプロバイダであるが、インターネットに接続されたその他のエンティティがリテーラの代わりに依頼を行ったりプロバイダの代わりに依頼を受けたりする場合には、リテ



ーラやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【0190】

仲介許諾証依頼のデータ構造を以下に示す。

【0191】

【表 8】

仲介許諾証依頼 ::= {

発信者フィールド,  
受信者フィールド,  
日時フィールド,  
仲介許諾仕様フィールド,  
デジタル署名フィールド,  
証明証フィールド

}

【0192】

発信者フィールド：この仲介許諾証依頼の発信者の識別子が記載される。発信者は通常リテーラであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この仲介許諾証依頼の受信者の識別子が記載される。受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この仲介許諾証依頼の作成日時が記載される。

仲介許諾仕様フィールド：作成してもらう仲介許諾証に対する依頼者の要望を記載した仲介許諾仕様が記載される。

デジタル署名フィールド：この仲介許諾証依頼の発信者によるこの仲介許諾証依頼に対するデジタル署名が記載される。

証明証フィールド：この仲介許諾証依頼のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0193】

仲介許諾証依頼の仲介許諾仕様フィールドに記載される仲介許諾仕様のデータ

構造を以下に示す。

【0194】

【表9】

仲介許諾仕様：：＝ {

許諾者フィールド，  
被許諾者フィールド，  
公開鍵識別子フィールド，  
希望利用条件限定情報フィールド  
}

【0195】

許諾者フィールド：仲介許諾証を作成してほしいプロバイダの識別子が記載される。

被許諾者フィールド：希望する仲介許諾証によって許諾を受けるリテーラの識別子が記載される。

公開鍵識別子フィールド：仲介許諾証で利用許可証の仲介を許諾してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

希望利用条件限定情報フィールド：作成してもらう仲介許諾証に記載してほしい利用条件限定情報が記載される。

【0196】

仲介許諾証依頼を受け取ったプロバイダは、仲介許諾証依頼に記載された仲介許諾仕様にしたがって仲介許諾証を作成し、リテーラに渡す。依頼された仲介許諾証を作成するかしないか、あるいは、指定された仲介許諾仕様どおりに仲介許諾証を作成するかどうかはプロバイダが決定できる。

【0197】

作成した仲介許諾証を引き渡す際には、仲介許諾証送付というデータが送受信される。通常、発信者は仲介許諾証を作成したプロバイダであり、受信者は発行された仲介許諾証を使用するリテーラであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに仲介許諾証の送付を行ったり、リテーラの代わりに仲介許諾証を受け取ったりする場合には、プロバイダやリテーラ

以外のエンティティが発信者や受信者になってもよい。

【0198】

仲介許諾証送付のデータ構造を以下に示す。

【0199】

【表10】

仲介許諾証送付 ::= {

発信者フィールド,  
受信者フィールド,  
日時フィールド,  
仲介許諾証フィールド,  
デジタル署名フィールド,  
証明証フィールド

}

【0200】

発信者フィールド：この仲介許諾証送付の送付者の識別子が記載される。発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この仲介許諾証送付の受信者の識別子が記載される。受信者は通常リテラであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この仲介許諾証送付の作成日時が記載される。

仲介許諾証フィールド：この仲介許諾証送付で送られる仲介許諾証が記載される。

デジタル署名フィールド：この仲介許諾証送付の発信者によるこの仲介許諾証送付に対するデジタル署名が記載される。

証明証フィールド：この仲介許諾証送付のデジタル署名フィールド、およびこの仲介許諾証送付に含まれる仲介許諾証のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0201】

### [利用許可証の発行]

利用許可証は、消費者からの依頼に応じて発行される。消費者はリテーラに対して特定のデジタルコンテンツに対して特定の利用条件での予約を依頼する利用許可証依頼を送付する。利用許可証依頼を受け取ったリテーラは、通常センタに対して、依頼元である消費者に対する利用許可証の発行を依頼するため利用許可証依頼を作成し、センタに送付する。利用許可証依頼を受け取ったセンタは消費者向けの利用許可証を作成し、利用許可証依頼を送付してきたリテーラに渡す。利用許可証を受け取ったリテーラは、その利用許可証をその依頼者である消費者に送付する。センタからあるいはリテーラからの利用許可証の送付には、利用許可証送付というデータが送受信される。

#### 【0202】

消費者とセンタの間を複数のリテーラが仲介することも可能である。その場合、消費者からの依頼を直接受けたリテーラが第2のリテーラに利用許可証依頼を送付し、第2のリテーラがセンタに利用許可証依頼を送付するという形態をとる。発行された利用許可証は逆の経路で利用許可証送付を送付していく事で消費者に届いてもよいし、いくつかのリテーラをスキップしてもよい。

#### 【0203】

利用許可証依頼のデータ構造を以下に示す。

#### 【0204】

#### 【表11】

```
利用許可証依頼 ::= {
    発信者フィールド,
    受信者フィールド,
    日時フィールド,
    許可内容フィールド,
    デジタル署名フィールド,
    証明証フィールド
}
```

#### 【0205】

発信者フィールド：この利用許可証依頼の発信者の識別子が記載される。

受信者フィールド：この利用許可証依頼の受信者の識別子が記載される。

日時フィールド：この利用許可証依頼の作成日時が記載される。

許可内容フィールド：依頼する利用許可証の内容に関する要望のためのフィールドである。通常、利用許可に関する要望を記した許可仕様が記載されるが、受信者がリテーラであって、リテーラで販売している物品あるいはサービスにリテーラ独自の管理番号が割り当ててある場合には、その番号が記載されることもある。

デジタル署名フィールド：この利用許可証依頼の発信者によるこの利用許可証依頼に対するデジタル署名が記載される。

証明証フィールド：この利用許可証依頼のデジタル署名フィールド、およびこの利用許可証依頼に仲介許諾が含まれるならばそのデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

#### 【0206】

利用許可証依頼の許可内容フィールドに記載される許可仕様のデータ構造を以下に示す。

#### 【0207】

#### 【表12】

許可仕様：：＝ {

公開鍵識別子フィールド，  
消費者識別子フィールド，  
利用条件フィールド，  
仲介許諾証フィールド  
}

#### 【0208】

#### 【表13】

公開鍵識別子フィールド：利用許可証依頼で依頼する利用許可証を検証できる検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

消費者識別子フィールド：利用許可証依頼で依頼する利用許可証で予約を証され

る消費者の識別子が記載される。

利用条件フィールド：利用許可証依頼で依頼する利用許可証に記載してほしい利用条件が記載される。

仲介許諾証フィールド：利用許可証依頼の発信者がリテラの場合に、そのリテラが、この許可仕様の公開鍵識別子フィールドに指定された識別子をもつ検証用公開鍵に対応する利用許可証を、この許可仕様の利用条件フィールドに記載された利用条件で仲介することが許諾されている事を証する仲介許諾証が含まれる。

#### 【0209】

許可仕様の利用条件フィールドに記載されたとおりの利用条件を持つ利用許可証を発行するかどうかは、センタが決定する。特に、許可仕様に含まれる仲介許諾証で許諾されていない依頼に対しては、利用許可証を発行しない。

#### 【0210】

また、利用許可証の依頼の過程で、仲介するリテラが許可仕様の利用条件フィールドの内容を修正する事もありうる。

#### 【0211】

利用許可証送付のデータ構造を以下に示す。

#### 【0212】

#### 【表14】

利用許可証送付：：＝ {

発信者フィールド，  
受信者フィールド，  
日時フィールド，  
利用許可証フィールド，  
デジタル署名フィールド，  
証明証フィールド  
}

#### 【0213】

発信者フィールド：この利用許可証送付の送付者の識別子が記載される。

受信者フィールド：この利用許可証送付の受信者の識別子が記載される。

日時フィールド：この利用許可証送付の作成日時が記載される。

利用許可証フィールド：この利用許可証送付で送られる利用許可証が記載される。

デジタル署名フィールド：この利用許可証送付の発信者によるこの仲介許諾送付に対するデジタル署名が記載される。

証明証フィールド：この利用許可証送付のデジタル署名フィールド、およびこの利用許可証送付に含まれる利用許可証のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

#### 【 0 2 1 4 】

##### [センタの構成]

本実施例のセンタは、インターネットを介して入力される検証用公開鍵情報依頼と利用許可証依頼を処理する機能、利用許可証の発行履歴を作成してインターネットを介してプロバイダあるいはリテーラに送付する機能、検証用公開鍵情報の発行履歴を作成してインターネットを介してプロバイダに送付する機能を持つ。

#### 【 0 2 1 5 】

図 2 は、本実施例のセンタの構成図である。

#### 【 0 2 1 6 】

センタは、入出力制御部 2 0 1、処理選択部 2 0 2、検証用公開鍵情報依頼処理部 2 0 3、利用許可証依頼処理部 2 0 4、プロバイダ DB 2 0 5、公開鍵ペア DB 2 0 6、リテーラ DB 2 0 7、消費者 DB 2 0 8、利用許可証発行履歴 DB 2 0 9、署名鍵記憶部 2 1 0、証明証記憶部 2 1 1、利用許可証発行プロバイダ用履歴作成部 2 1 2、利用許可証発行リテーラ用履歴作成部 2 1 3、検証用公開鍵情報発行履歴作成部 2 1 4 から構成され、入出力制御部 2 0 1 を介してインターネットに接続されている。

#### 【 0 2 1 7 】

本実施例のセンタの各部の役割を以下に述べる。

#### 【 0 2 1 8 】

入出力制御部 201 : インターネットを介したデータの入力を受け付けるとともに、検証用公開鍵情報依頼処理部 203 が作成したデータや利用許可証依頼処理部 204 が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部 201 への入力、あるいは、入出力制御部 201 からインターネットへの出力の方法としては、入出力制御部 201 と接続された WWW サイトを準備してプロバイダやリテーラにアクセスさせるもの、あるいは電子メールシステムと入出力制御部 201 を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部 202 : 入力したデータが検証用公開鍵情報依頼かまたは利用許可証依頼かを判断し、検証用公開鍵情報依頼であれば検証用公開鍵情報依頼処理部 203 を、利用許可証依頼であれば利用許可証依頼処理部 204 を呼び出す。

検証用公開鍵情報依頼処理部 203 : 検証用公開鍵情報依頼を処理し、検証用公開鍵情報依頼送付を作成して入出力制御部 201 を介して依頼者に送付する。検証用公開鍵情報依頼送付作成の過程で、プロバイダ DB 205 を参照し、公開鍵ペア DB 206 に新しいエントリを追加する。

利用許可証依頼処理部 204 : 利用許可証依頼を処理し、利用許可証依頼送付を作成して入出力制御部 201 を介して依頼者に送付する。利用許可証依頼送付作成の過程で、公開鍵ペア DB 206、リテーラ DB 207、消費者 DB 208 を参照し、利用許可証発行履歴 DB 209 に新しいエントリを追加する。

プロバイダ DB 205 : プロバイダに関するデータを保持する DB。

公開鍵ペア DB 206 : 利用許可証の作成に使用される公開鍵ペアに関する情報を保持する DB。

リテーラ DB 207 : リテーラに関するデータを保持する DB。

消費者 DB 208 : 消費者に関するデータを保持する DB。

利用許可証発行履歴 DB 209 : 利用許可証の発行履歴に関するデータを保持する DB。

署名鍵記憶部 210 : センタが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部 211 : 署名鍵記憶部 210 に記憶されている署名鍵で作成したデ



デジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

利用許可証発行プロバイダ用履歴作成部 212：各プロバイダ毎の利用許可証の発行履歴を作成し、入出力制御部 201 を介してプロバイダに送付する。

利用許可証発行リテーラ用履歴作成部 213：各リテーラ毎の利用許可証の発行履歴を作成し、入出力制御部 201 を介してリテーラに送付する。

検証用公開鍵情報発行履歴作成部 214：各プロバイダ毎の検証用公開鍵情報の発行履歴を作成し、入出力制御部 201 を介してプロバイダに送付する。

#### 【0219】

[センタが持つデータベース]

センタは、プロバイダDB 205、公開鍵ペアDB 206、リテーラDB 207、消費者DB 208、利用許可証発行履歴DB 209の5つのデータベースを持っている。

#### 【0220】

プロバイダDB 205は、センタがプロバイダとして認めているエンティティに関する情報を保持したデータベースである。

#### 【0221】

プロバイダDB 205の構造を図6に示す。プロバイダDB 205は以下の唯一の属性からなるテーブルである。

#### 【0222】

【表15】

プロバイダ識別子属性：センタがプロバイダとして認めているエンティティの識別子。

#### 【0223】

センタは、このデータベースに登録されているプロバイダ以外のエンティティをプロバイダとは認めない。したがって、そのようなエンティティに対して検証用公開鍵情報を発行することはないし、そのようなエンティティが提供しているデジタルコンテンツに対する利用許可証を発行する事もない。

#### 【0224】

センタがプロバイダと認めるエンティティを増やしたい場合には、このデータ

ベースに新規エントリを追加する。

【0225】

公開鍵ペアDB206は、プロバイダに発行される検証用公開鍵と、それに対応する秘密鍵に関する情報を保持したデータベースである。本実施例では、検証用公開鍵とそれに対応する秘密鍵のための公開鍵暗号アルゴリズムとしてRSAを使用する。したがって、公開鍵ペアDB206はRSAの公開鍵ペアについての情報を保持するデータベースである。

【0226】

公開鍵ペアDB206の構造を図7に示す。公開鍵ペアDB206は以下の7つの属性からなるテーブルであり、各エントリはそれぞれ一つの公開鍵ペアに関する情報である。

【0227】

【表16】

公開鍵識別子属性：このエントリの公開鍵ペアに割り当てられた検証用公開鍵識別子。

法数属性：RSA法数。

公開鍵属性：RSA公開鍵。

秘密鍵属性：RSA秘密鍵。

プロバイダ識別子属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報を発行されたプロバイダの識別子。

有効期間開始属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の終了日時。

発行日属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の発行日時。

【0228】

リテラDB207は、センタがリテラとして認めているエンティティに関する情報を保持したデータベースである。

## 【0229】

リテラDB207の構造を図8に示す。リテラDB207は以下の唯一の属性からなるテーブルである。

## 【0230】

## 【表17】

リテラ識別子属性：センタがリテラとして認めているエンティティの識別子

。

## 【0231】

センタは、このデータベースに登録されているリテラ以外のエンティティをリテラとは認めない。したがって、そのようなエンティティからの利用許可証発行依頼に対して利用許可証を発行する事はない。

## 【0232】

センタがリテラと認めるエンティティを増やしたい場合には、このデータベースに新規エントリを追加する。

## 【0233】

消費者DB208は、センタが消費者として認めているエンティティに関する情報を保持したデータベースである。

## 【0234】

消費者DB208の構造を図9に示す。消費者DB208は以下の2つの属性からなるテーブルである。

## 【0235】

## 【表18】

消費者識別子属性：センタが消費者として認めている消費者識別子。

消費者秘密情報属性：消費者識別子属性で指定された消費者識別子に対応する消費者秘密情報。

## 【0236】

利用許可証発行履歴DB209は、センタがこれまでに発行した利用許可証に関する情報を保持したデータベースである。

## 【0237】

利用許可証発行履歴DB209の構造を図10に示す。消費者DB208は以下の6つの属性からなるテーブルであり、各エントリはそれぞれ一つの利用許可証に関する情報である。

#### 【0238】

##### 【表19】

公開鍵識別子属性：このエントリの利用許可証を検証できる検証用公開鍵に割り当てられた検証用公開鍵識別子。

プロバイダ識別子属性：このエントリの公開鍵識別子属性で指定された検証用公開鍵を含む検証用公開鍵情報の発行を受けたプロバイダの識別子。

消費者識別子属性：このエントリ利用許可証でデジタルコンテンツの利用を許可された消費者の消費者識別子。

仲介者識別子属性：このエントリ利用許可証の発行を依頼したリテーラの識別子。

利用条件属性：このエントリ利用許可証に記載された利用条件をBER (Basic Encoding Rule: ITU-T Recommendation X.690) にしたがってエンコードした結果。

発行日属性：このエントリ利用許可証の発行日時。

#### 【0239】

図3は、本実施例のセンタの動作を示すフローチャートである。本実施例のセンタの動作を図3のフローチャートにしたがって説明する。

#### 【0240】

図3に示す通り、本実施例のセンタは、データの入力を待ち続け、入力があれば入力に応じた処理を行った後に再度入力待ちの状態に戻る終わる事のない処理である。

#### 【0241】

最初に、入出力制御部201で入力があるかどうかチェックされる(301)。ここで入力がなければ、再度入力のチェック(301)に戻る。

#### 【0242】

入力のチェック(301)で入力があった場合、処理選択部202で、その入

力が検証用公開鍵情報依頼かどうか判断される（302）。入力検証用公開鍵情報依頼であれば、検証用公開鍵情報依頼処理部203が呼び出され検証用公開鍵情報依頼が処理される（303）。検証用公開鍵情報依頼の処理が終われば、再度入力のチェック（301）に戻る。

#### 【0243】

302の判断で、入力検証用公開鍵情報依頼でなければ、処理選択部202で、その入力利用許可証依頼かどうか判断される（304）。入力利用許可証依頼であれば、利用許可証依頼処理部204が呼び出され利用許可証依頼が処理される（305）。利用許可証依頼の処理が終われば、再度入力のチェック（301）に戻る。

#### 【0244】

また、304の判断で、入力利用許可証依頼でなければ、再度入力のチェック（301）に戻る。

#### 【0245】

#### 〔検証用公開鍵情報依頼処理部〕

図4は、本実施例のセンタが持つ検証用公開鍵情報依頼処理部203の内部構成を示した図である。

#### 【0246】

検証用公開鍵情報依頼処理部203は、検証用公開鍵情報依頼を処理する機能を持ち、処理制御部401、署名検証部402、公開鍵ペア作成部403、公開鍵ペア識別子作成部404、検証用公開鍵情報作成部405、検証用公開鍵情報送付作成部406、エラーメッセージ作成部407、署名作成部408から構成される。

#### 【0247】

検証用公開鍵情報依頼処理部203を構成する各部の役割を以下に述べる。

#### 【0248】

処理制御部401：処理選択部202からの入力、入出力制御部201への出力、プロバイダDB205の参照、公開鍵ペアDB206へのエントリの追加の機能を担うとともに、検証用公開鍵情報依頼の処理全体を制御する。

署名検証部402：処理選択部202から入力される検証用公開鍵情報依頼のデジタル署名を検証する。

公開鍵ペア作成部403：検証用公開鍵および利用許可証の作成に使用される公開鍵ペアを作成する。

公開鍵ペア識別子作成部404：検証用公開鍵に割り当てられる検証用公開鍵識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

検証用公開鍵情報作成部405：検証用公開鍵情報を作成する。検証用公開鍵情報にデジタル署名を添付するために署名作成部408を呼び出す。

検証用公開鍵情報送付作成部406：検証用公開鍵情報送付を作成する。検証用公開鍵情報送付にデジタル署名を添付するために署名作成部408を呼び出す。さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部211にアクセスする。

エラーメッセージ作成部407：エラーメッセージを作成する。

署名作成部408：検証用公開鍵情報、検証用公開鍵情報送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部210にアクセスする。

#### 【0249】

図5は、本実施例のセンタが持つ検証用公開鍵情報依頼処理部203の処理制御部401の動作を示すフローチャートである。処理制御部401の動作を図5にしたがって説明する。

#### 【0250】

まず、処理選択部202から入力された検証用公開鍵情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子を取り出し、センタがこの識別子のエンティティをプロバイダとして認めているかどうかをプロバイダDB205を参照して調べる(501)。プロバイダDB205にこの識別子を持つエントリが存在すれば、プロバイダとして認めたエンティティであることがわかる。

#### 【0251】

501の判断で、プロバイダとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部407でエラーメッセージを作成して入出力制御部201に出力した後(509)、終了する。

【0252】

501の判断で、プロバイダとして認めているエンティティであることがわかった場合、検証用公開鍵情報依頼のデジタル署名を検証する(502)。検証鍵は検証用公開鍵情報依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA108から公開鍵証明証を取得してから署名の検証を行う。

【0253】

署名の検証に失敗した場合、エラーメッセージ作成部407でエラーメッセージを作成して入出力制御部201に出力した後(509)、終了する。

【0254】

署名の検証に成功した場合、公開鍵ペア作成部403を呼び出してRSA公開鍵ペアを作成させ、作成された法数、公開鍵、秘密鍵を受け取る(503)。さらに、公開鍵ペア識別子作成部404を呼び出して検証用公開鍵情報に割り当てる識別子を作成させ、作成された識別子を受け取る(504)。

【0255】

次に検証用公開鍵情報の有効期間の開始日時と終了日時を適切に決定した後(505)、新しいエントリを公開鍵ペアDBに追加する(506)。新しいエントリの各属性には以下の値が設定される。

【0256】

【表20】

公開鍵識別子属性：504で作成した識別子。

法数属性：503で作成したRSA法数。

公開鍵属性：503で作成したRSA公開鍵。

秘密鍵属性：503で作成したRSA秘密鍵。

プロバイダ識別子属性：検証用公開鍵情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

有効期間開始属性：5 0 5 で作成した有効期間の開始日時。

有効期間終了属性：5 0 5 で作成した有効期間の終了日時。

発行日属性：現在の日時。

#### 【0 2 5 7】

次に、検証用公開鍵情報作成部（4 0 5）を呼び出し、検証用公開鍵情報を作成させ、その結果を受け取る（5 0 7）。検証用公開鍵情報の各フィールドには以下の値が設定される。

#### 【0 2 5 8】

##### 【表 2 1】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：検証用公開鍵情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

発行日フィールド：現在の時刻。

有効期間開始日時フィールド：5 0 5 で作成した有効期間の開始日時。

有効期間終了日時フィールド：5 0 5 で作成した有効期間の終了日時。

検証用公開鍵識別子フィールド：5 0 4 で作成した識別子。

公開鍵情報フィールド：5 0 3 で作成した法数、公開鍵、秘密鍵。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部 4 0 8 を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

#### 【0 2 5 9】

最後に、検証用公開鍵情報送付作成部 4 0 6 を呼び出し、検証用公開鍵情報送付を作成させ、その結果を受け取って入出力制御部 2 0 1 に出力した後（5 0 8）、終了する。検証用公開鍵情報送付の各フィールドには以下の値が設定される。

#### 【0 2 6 0】

##### 【表 2 2】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：検証用公開鍵情報依頼の発信者フィールドに記載されている



識別子。

日時フィールド：現在の時刻。

検証用公開鍵情報フィールド：507で作成した検証用公開鍵情報。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部408を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部211に記憶している公開鍵証明証。

#### 【0261】

##### [利用許可証依頼処理部]

図11は、本実施例のセンタが持つ利用許可証依頼処理部204の内部構成を示した図である。

#### 【0262】

利用許可証依頼処理部204は、利用許可証依頼を処理する機能を持ち、処理制御部1101、署名検証部1102、仲介許諾内容確認部1103、利用許可証識別子作成部1104、利用許可証作成部1105、利用許可証送付作成部1106、エラーメッセージ作成部1107、署名作成部1108、証明値作成部1109、利用条件作成部1110から構成される。

#### 【0263】

利用許可証依頼処理部204を構成する各部の役割を以下に述べる。

#### 【0264】

処理制御部1101：処理選択部202からの入力、入出力制御部201への出力、公開鍵ペアDB206リテラDB207消費者DB208の参照、利用許可証発行履歴DB209へのエントリの追加の機能を担うとともに、利用許可証依頼の処理全体を制御する。

署名検証部1102：処理選択部202から入力される利用許可証依頼、および該利用許可証依頼に含まれる仲介許諾証のデジタル署名を検証する。

仲介許諾内容確認部1103：処理選択部202から入力される利用許可証依頼で依頼された利用許可証の仲介が、該利用許可証依頼に含まれている仲介許諾証によって許諾されているかどうかを確認する。

利用許可証識別子作成部 1104：利用許可証に割り当てられる利用許可証識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

利用許可証作成部 1105：利用許可証を作成する。利用許可証にデジタル署名を添付するために署名作成部 1108 を呼び出す。

利用許可証送付作成部 1106：利用許可証送付を作成する。利用許可証送付にデジタル署名を添付するために署名作成部 1108 を呼び出す。さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 211 にアクセスする。

エラーメッセージ作成部 1107：エラーメッセージを作成する。

署名作成部 1108：利用許可証、利用許可証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 210 にアクセスする。

証明値作成部 1109：利用許可証に含まれる証明値を作成する。

利用条件作成部 1110：利用許可証に含まれる利用条件を作成する。

#### 【0265】

図 12 は、本実施例のセンタが持つ利用許可証依頼処理部 204 の処理制御部 1101 の動作を示すフローチャートである。処理制御部 1101 の動作を図 12 にしたがって説明する。

#### 【0266】

まず、処理選択部 202 から入力された利用許可証依頼の発信者フィールドに記載されている識別子を取り出し、センタがこの識別子のエンティティをリテラとして認めているかどうかをリテラ DB 207 を参照して調べる（1201）。リテラ DB 207 にこの識別子を持つエントリが存在すれば、リテラとして認めたエンティティであることがわかる。

#### 【0267】

1201 の判断で、リテラとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部 1107 でエラーメッセージを作成して入出力制御部 201 に出力した後（1210）、終了する。

## 【0268】

1201の判断で、リテラとして認めているエンティティであることがわかった場合、利用許可証依頼のデジタル署名、および利用許可証依頼に含まれる仲介許諾証のデジタル署名を検証する(1202)。検証鍵は利用許可証依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA108から公開鍵証明証を取得してから署名の検証を行う。

## 【0269】

署名の検証に失敗した場合、エラーメッセージ作成部1107でエラーメッセージを作成して入出力制御部201に出力した後(1210)、終了する。

## 【0270】

署名の検証に成功した場合、利用許可証依頼で依頼された利用許可証の仲介が、該利用許可証依頼に含まれている仲介許諾証によって許諾されているかどうかを確認する(1203)。より具体的には、利用許可証依頼の許可内容フィールドに含まれている許可仕様を仲介許諾内容確認部1103に送付し、該許可仕様の公開鍵鍵識別子フィールドで指定されている検証用公開鍵識別子を持つ検証用公開鍵に対応する利用許可証を、該許可仕様の利用条件フィールドに記載されている利用条件で発行することが、該許可仕様の仲介許諾証フィールドに含まれている仲介許諾証で許諾されているかどうかを確認する。

## 【0271】

1203で、許諾されていない事がわかった場合、エラーメッセージ作成部1107でエラーメッセージを作成して入出力制御部201に出力した後(1210)、終了する。

## 【0272】

1203で、許諾されている事がわかった場合、利用許可証識別子作成部1104を呼び出して利用許可証に割り当てる識別子を作成させ、作成された識別子を受け取った後(1204)、利用条件作成部1110を呼び出して、利用許可証に記載する利用条件を決定する(1205)。利用条件作成部が生成する利用条件は、利用許可証依頼の許可内容フィールドに含まれている許可仕様の利用条

件フィールドの値そのままでもよいし、該許可仕様の仲介許諾証フィールドに含まれている仲介許諾証によって許諾されている範囲内で該利用条件フィールドの値を適切に修正したものであってもよい。

#### 【0273】

利用条件の作成の後、新しいエントリを利用許可証発行履歴DB209に追加する(1206)。新しいエントリの各属性には以下の値が設定される。

#### 【0274】

##### 【表23】

公開鍵識別子属性：利用許可証依頼の許可内容フィールドに含まれている許可仕様の公開鍵識別子フィールドの値。

プロバイダ識別子属性：公開鍵ペアDBにアクセスし、該公開鍵ペアDBの公開鍵識別子属性が、利用許可証依頼の許可内容フィールドに含まれている許可仕様の公開鍵識別子フィールドの値と同じ値を持つエントリの、プロバイダ識別子属性を取り出し、その値を設定する。

消費者識別子属性：利用許可証依頼の許可内容フィールドに含まれている許可仕様の消費者識別子フィールドの値。

仲介者識別子属性：利用許可証依頼の発信者フィールドの値。

利用条件属性：1205で利用条件作成部が作成した利用条件。

発行日属性：現在の日時。

#### 【0275】

次に、証明値作成部1109を呼び出して証明値を作成させ、その結果を受け取る(1207)。さらに、利用許可証作成部1105を呼び出し、利用許可証を作成させ、その結果を受け取る(1208)。利用許可証の各フィールドには以下の値が設定される。

#### 【0276】

##### 【表24】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：利用許可証依頼の許可内容フィールドに含まれている許可仕様の消費者識別子フィールドの値。

発行日フィールド：1206で利用許可証発行履歴DB209に追加したエントリの発行日属性の値。

利用許可証識別子フィールド：1204で作成した識別子。

公開鍵識別子フィールド：利用許可証依頼の許可内容フィールドに含まれている許可仕様の公開鍵識別子フィールドの値。

利用条件フィールド：1205で利用条件作成部が作成した利用条件。

証明値フィールド：1207で作成した証明値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1108を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

#### 【0277】

最後に、利用許可証送付作成部1106を呼び出し、利用許可証送付を作成させ、その結果を受け取って入出力制御部201に出力した後（1209）、終了する。利用許可証送付の各フィールドには以下の値が設定される。

#### 【0278】

##### 【表25】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：利用許可証依頼の発信者フィールドの値。

日時フィールド：現在の時刻。

利用許可証フィールド：1208で作成した利用許可証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1108を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部211に記憶している公開鍵証明証。

#### 【0279】

##### 【センタが持つその他の機能】

本実施例のセンタは、利用許可証発行の履歴情報をプロバイダに送付することができる。

#### 【0280】

プロバイダに渡される利用許可証発行の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する利用許可証の発行についての情報であり、利用許可証発行プロバイダ用履歴作成部 2 1 2 で作成され、入出力制御部 2 0 1 を介してプロバイダに送付される。プロバイダにとっては、この履歴情報は、自己が提供しているデジタルコンテンツをどのリテーラがどのぐらい販売したかのを示す信頼できる情報であり、販売におけるマージンがリテーラからプロバイダに渡される場合に、リテーラから送られたマージンの正しさをプロバイダが確認する際の重要な情報となる。

#### 【 0 2 8 1 】

利用許可証発行プロバイダ用履歴作成部 2 1 2 は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証発行履歴 DB 2 0 9 から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、仲介者識別子属性、利用条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

#### 【 0 2 8 2 】

本実施例のセンタは、利用許可証発行の履歴情報をリテーラにも送付することができる。

#### 【 0 2 8 3 】

リテーラに渡される利用許可証発行の履歴情報は、そのリテーラからの依頼で行った利用許可証の発行についての情報であり、利用許可証発行リテーラ用履歴作成部 2 1 3 で作成され、入出力制御部 2 0 1 を介してリテーラに送付される。この履歴は、センタがリテーラから利用許可証発行のマージンを受け取る場合のマージンの額の根拠となる。

#### 【 0 2 8 4 】

利用許可証発行リテーラ用履歴作成部 2 1 3 は、履歴を作成するリテーラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証発行

履歴DB 209から、仲介者識別子属性の値が指定されたりテラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、利用条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するリテラの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でリテラから入力されるように構成してもよい。

## 【0285】

また、本実施例のセンタは、検証用公開鍵情報発行の履歴情報をプロバイダに送付する事ができる。

## 【0286】

プロバイダに渡される検証用公開鍵情報発行の履歴情報は、そのプロバイダに対して発行された検証用公開鍵情報についての情報であり、検証用公開鍵情報発行履歴作成部214で作成され、入出力制御部201を介してプロバイダに送付される。この履歴は、センタがプロバイダから検証用公開鍵情報発行の手数料を徴収する場合の根拠となる。

## 【0287】

検証用公開鍵情報発行履歴作成部214は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、公開鍵ペアDB 206から、公開鍵識別子属性、法数属性、公開鍵属性、有効期間開始属性、有効期間終了属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

## 【0288】

上記の履歴情報のプロバイダやリテラへの送付方法は、電子メールでもよいし、WWWベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

## 【0289】

## [プロバイダの構成]

図 1 3 は、本実施例のプロバイダの構成図である。

### 【0290】

本実施例のプロバイダは、検証用公開鍵情報依頼を作成してインターネットを介してセンタに送付する機能と、インターネットを介して入力される検証用公開鍵情報送付と仲介許諾証依頼とを処理する機能を持つ。プロバイダは、入出力制御部 1 3 0 1、処理選択部 1 3 0 2、検証用公開鍵情報依頼作成部 1 3 0 3、検証用公開鍵情報送付処理部 1 3 0 4、仲介許諾証依頼処理部 1 3 0 5、検証用公開鍵 DB 1 3 0 6、署名鍵記憶部 1 3 0 7、証明証記憶部 1 3 0 8、仲介許諾証発行履歴 DB 1 3 0 9、仲介許諾証発行履歴作成部 1 3 1 0 から構成され、入出力制御部 1 3 0 1 を介してインターネットに接続されている。

### 【0291】

本実施例のプロバイダの各部の役割を以下に述べる。

### 【0292】

入出力制御部 1 3 0 1：インターネットを介したデータの入力を監視するとともに、検証用公開鍵情報依頼作成部 1 3 0 3 や仲介許諾証依頼処理部 1 3 0 5 が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部 1 3 0 1 への入力、あるいは、入出力制御部 1 3 0 1 からインターネットへの出力の方法としては、入出力制御部 1 3 0 1 と接続された WWW サイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意している WWW サイトにアクセスしてプロバイダが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部 1 3 0 1 を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部 1 3 0 2：入力したデータが検証用公開鍵情報送付かまたは仲介許諾証依頼かを判断し、検証用公開鍵情報送付であれば検証用公開鍵情報送付処理部 1 3 0 4 を、仲介許諾証依頼であれば仲介許諾証依頼処理部 1 3 0 5 を呼び出す。

検証用公開鍵情報依頼作成部 1 3 0 3：検証用公開鍵情報依頼を作成し、入出力制御部 1 3 0 1 を介してセンタに送付する。検証用公開鍵情報依頼作成の過程で



、署名鍵記憶部1307と証明証記憶部1308にアクセスする。

検証用公開鍵情報送付処理部1304：検証用公開鍵情報送付を処理し、検証用公開鍵を検証用公開鍵DB1306に登録する。

仲介許諾証依頼処理部1305：仲介許諾証依頼を処理し、仲介許諾証送付を作成して入出力制御部1301を介して依頼者に送付する。仲介許諾証送付作成の過程で検証用公開鍵DB1306を参照するとともに、仲介許諾発行履歴DB1309に新しいエントリを追加し、署名鍵記憶部1307と証明証記憶部1308にアクセスする。

検証用公開鍵DB1306：検証用公開鍵に関する情報を保持するDB。

署名鍵記憶部1307：プロバイダが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部1308：署名鍵記憶部1307に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

仲介許諾証発行履歴DB1309：仲介許諾証の発行の履歴を保持するDB。

仲介許諾証発行履歴作成部1310：リテラ毎の仲介許諾証の発行履歴を作成する。

#### 【0293】

[プロバイダが持つデータベース]

プロバイダは、検証用公開鍵DB1306、仲介許諾証発行履歴DB1309の2つのデータベースを持っている。

#### 【0294】

検証用公開鍵DB1306は、センタから発行を受けた検証用公開鍵情報の内容を、プロバイダ自身が決定した検証用公開鍵の用途とともに保持するデータベースである。

#### 【0295】

検証用公開鍵DB1306の構造を図14に示す。検証用公開鍵DB1306は以下の6つの属性からなるテーブルであり、各エントリはそれぞれ一つの検証用公開鍵に関する情報である。

#### 【0296】

## 【表 2 6】

公開鍵識別子属性：検証用公開鍵に割り当てられた検証用公開鍵識別子。

法数属性：検証用公開鍵情報に含まれていた R S A 法数。

公開鍵属性：検証用公開鍵情報に含まれていた R S A 公開鍵。

有効期間開始属性：検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：検証用公開鍵情報の有効期間の終了日時。

用途属性：このエントリの検証用公開鍵に対してプロバイダが割り当てた用途。  
この検証用公開鍵で利用許可証の正当性を検証するデジタルコンテンツあるいは  
その機能の情報である。

## 【0 2 9 7】

仲介許諾証発行履歴 D B 1 3 0 9 は、プロバイダが発行した仲介許諾証に関する履歴を保持するデータベースである。

## 【0 2 9 8】

仲介許諾証発行履歴 D B 1 3 0 9 の構造を図 3 4 に示す。仲介許諾証発行履歴 D B 1 3 0 9 は以下の 7 つの属性からなるテーブルであり、各エントリはそれぞれ一回の仲介許諾証の発行に関する情報である。

## 【0 2 9 9】

## 【表 2 7】

仲介許諾証識別子属性：発行した仲介許諾証に割り当てられた識別子。

公開鍵識別子属性：発行した仲介許諾証で利用許可証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子。

リテラ識別子属性：発行した仲介許諾証で許諾をうけるリテラの識別子。

利用条件限定情報属性：発行した仲介許諾証に記載されている利用条件限定情報。  
有効期間開始属性：発行した仲介許諾証の有効期間の開始日時。

有効期間終了属性：発行した仲介許諾証の有効期間の終了日時。

発行日属性：発行した仲介許諾証の発行日時。

## 【0 3 0 0】

## [検証用公開鍵情報依頼作成部]

本実施例のプロバイダは、新たに販売を開始したいデジタルコンテンツが発生

した時に、そのデジタルコンテンツに割り当てる検証用公開鍵を含む検証用公開鍵情報の発行をセンタに依頼する。依頼の際には、検証用公開鍵情報依頼作成部 1303 において検証用公開鍵情報依頼を作成し、入出力制御部 1301 を介してセンタに送付する。

#### 【0301】

検証用公開鍵情報依頼作成部 1303 では、検証用公開鍵情報依頼の各フィールドに以下の値を設定する。

#### 【0302】

##### 【表 28】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の時刻。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する要望。検証用公開鍵の使用者として自分の識別子を記載し、さらに、要望する公開鍵暗号アルゴリズムと鍵長が記載される。本実施例では公開鍵暗号アルゴリズムとしては RSA のみが可能なので、公開鍵暗号アルゴリズムの値は RSA で固定である。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、検証用公開鍵情報依頼作成部 1303 は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部 1307 にアクセスして入手する。

証明証フィールド：証明証記憶部 1308 に記憶している公開鍵証明証。

#### 【0303】

##### 【検証用公開鍵情報送付処理部】

検証用公開鍵情報依頼作成部 1303 で検証用公開鍵情報依頼が作成されセンタに送付されると、その返信としてセンタから検証用公開鍵情報送付が送信されてくる。検証用公開鍵情報送付は、入出力制御部 1301 および処理選択部 1302 を経由して検証用公開鍵情報送付処理部 1304 へ送られ、そこで処理される。

## 【0304】

図15は、本実施例のプロバイダが持つ検証用公開鍵情報送付処理部1304の動作を示すフローチャートである。検証用公開鍵情報送付処理部1304の動作を図15にしたがって説明する。

## 【0305】

まず、処理選択部1302から入力された検証用公開鍵情報送付、および、該検証用公開鍵情報送付に含まれる検証用公開鍵情報のデジタル署名を検証する（1501）。検証鍵は検証用公開鍵情報送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA108から公開鍵証明証を取得してから署名の検証を行う。署名の検証のために、検証用公開鍵情報送付処理部1304はデジタル署名の検証を専門に行う署名検証部を含んでいる。

## 【0306】

1501で、デジタル署名の検証に失敗した場合、エラー処理を行った後（1505）、終了する。

## 【0307】

1501で、デジタル署名の検証に成功した場合、検証用公開鍵情報送付に含まれている検証用公開鍵情報の発行者がセンタであるかどうか調べられる（1502）。この検査は、検証用公開鍵情報の発行者フィールドに記載されている識別子がセンタのものであるかどうかで検査できる。

## 【0308】

1502の検査で、検証用公開鍵情報の発行者がセンタでなかった場合、エラー処理を行った後（1505）、終了する。

## 【0309】

1502の検査で、検証用公開鍵情報の発行者がセンタであったら、次に検証用公開鍵DB1306に新しいエントリを追加する（1503）。新しいエントリの各属性には以下の値が設定される。

## 【0310】

【表29】

公開鍵識別子属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の検証用公開鍵識別子フィールドの値。

法数属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたRSA法数。

公開鍵属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたRSA公開鍵。

有効期間開始属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の有効期間開始日時フィールドの値。

有効期間終了属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の有効期間終了日時フィールドの値。

用途属性：この検証用公開鍵にプロバイダ割り当てた用途についての情報。

#### 【0311】

##### [仲介許諾証依頼処理部]

図16は、本実施例のプロバイダが持つ仲介許諾証依頼処理部1305の内部構成を示した図である。

#### 【0312】

仲介許諾証依頼処理部1305は、仲介許諾証依頼を処理する機能を持ち、処理制御部1601、署名検証部1602、仲介許諾証識別子作成部1603、エラーメッセージ作成部1604、仲介許諾証作成部1605、仲介許諾証送付作成部1606、署名作成部1607、利用条件限定情報作成部1608から構成される。

#### 【0313】

仲介許諾証依頼処理部1305を構成する各部の役割を以下に述べる。

#### 【0314】

処理制御部1601：処理選択部1302からの入力、入出力制御部1301への出力、検証用公開鍵DB1306の参照、仲介許諾証発行履歴DB1309へのエントリの追加の機能を担うとともに、仲介許諾証依頼の処理全体を制御する。

署名検証部1602：処理選択部202から入力される仲介許諾証依頼のデジタ

ル署名を検証する。

仲介許諾証識別子作成部 1 6 0 3 : 仲介許諾証に割り当てられる仲介許諾証識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

エラーメッセージ作成部 1 6 0 4 : エラーメッセージを作成する。

仲介許諾証作成部 1 6 0 5 : 仲介許諾証を作成する。仲介許諾証にデジタル署名を添付するために署名作成部 1 6 0 7 を呼び出す。

仲介許諾証送付作成部 1 6 0 6 : 仲介許諾証送付を作成する。仲介許諾証送付にデジタル署名を添付するために署名作成部 1 6 0 7 を呼び出す。さらに、プロバイダの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 1 3 0 8 にアクセスする。

署名作成部 1 6 0 7 : 仲介許諾証、仲介許諾証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 1 3 0 7 にアクセスする。

利用条件限定情報作成部 1 6 0 8 : 仲介許諾証に記載される利用条件限定情報を作成する。

#### 【 0 3 1 5 】

図 1 7 は、本実施例のプロバイダが持つ仲介許諾証依頼処理部 1 3 0 5 の処理制御部 1 6 0 1 の動作を示すフローチャートである。処理制御部 1 6 0 1 の動作を図 1 7 にしたがって説明する。

#### 【 0 3 1 6 】

まず、処理選択部 1 3 0 2 から入力された仲介許諾証依頼のデジタル署名を検証する ( 1 7 0 1 ) 。検証鍵は仲介許諾証依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA 1 0 8 から公開鍵証明証を取得してから署名の検証を行う。

#### 【 0 3 1 7 】

署名の検証に失敗した場合、エラーメッセージ作成部 1 6 0 4 でエラーメッセージを作成して入出力制御部 1 3 0 1 に出力した後 ( 1 7 0 9 ) 、終了する。

#### 【 0 3 1 8 】

署名の検証に成功した場合、仲介許諾証依頼で依頼された仲介許諾証を発行するかどうかを決定する（1702）。仲介許諾証を発行するかどうかの決定はプロバイダにまかされている。例えば、仲介許諾証によって許諾を受けるリテラを信用できない場合や、仲介許諾証依頼に含まれる仲介許諾証仕様の許諾者フィールドに記載されている識別子が自分のものと異なる場合や、仲介許諾証依頼に含まれる仲介許諾仕様の公開鍵識別子フィールドに記載された検証用公開鍵識別子を持つ検証用公開鍵情報が自分に対して発行されたものでない場合や、仲介許諾証依頼に含まれる仲介許諾仕様の希望利用条件限定情報フィールドの希望にそえない場合に仲介許諾証の発行をやめることになる。

#### 【0319】

1702で、仲介許諾証を発行しないと決定した場合には、エラーメッセージ作成部1604でエラーメッセージを作成して入出力制御部1301に出力した後（1709）、終了する。

#### 【0320】

1702で、仲介許諾証を発行すると決定した場合には、仲介許諾証識別子作成部1603を呼び出して仲介許諾証に割り当てる識別子を作成させ、作成された識別子を受け取った後（1703）、発行する仲介許諾証の有効期間を適切に決定する（1704）。

#### 【0321】

さらに、利用条件限定情報作成部1608を呼び出して発行する仲介許諾証に含まれる利用条件限定情報を作成させ、その結果を受け取る（1705）。ここで作成する利用条件限定情報は、仲介許諾証依頼に含まれる仲介許諾仕様の希望利用条件限定情報フィールドに記載されているものでもよいし、プロバイダが自己の判断で適切な利用条件限定情報を決定してもよい。

#### 【0322】

その後、仲介許諾証作成部1605を呼び出し、仲介許諾証を作成させ、その結果を受け取る（1706）。仲介許諾証の各フィールドには以下の値が設定される。

#### 【0323】

## 【表 30】

発行者フィールド：自分自身すなわちプロバイダの識別子。

受領者フィールド：仲介許諾証依頼に含まれる仲介許諾仕様の被許諾者フィールドの値。

発行日フィールド：現在の日時。

仲介許諾証識別子フィールド：1703で作成した識別子。

有効期間開始日時フィールド：1704で決定した有効期間の開始日時。

有効期間終了日時フィールド：1704で決定した有効期間の終了日時。

公開鍵識別子フィールド：仲介許諾証依頼に含まれる仲介許諾仕様の公開鍵識別子フィールドの値。

利用条件限定情報フィールド：1705で決定した利用条件限定情報の値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1607を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

## 【0324】

次に、仲介許諾証送付作成部1606を呼び出し、仲介許諾証送付を作成させ、その結果を受け取って入出力制御部1301に出力する（1707）。仲介許諾証送付の各フィールドには以下の値が設定される。

## 【0325】

## 【表 31】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：仲介許諾証依頼の発信者フィールドに記載されている識別子。

日時フィールド：現在の日時。

仲介許諾証フィールド：1706で作成した仲介許諾証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1607を呼び出し、結果の署名値をこのフィールドに設定する。

## 【0326】



## 【表 3 2】

証明証フィールド：証明証記憶部 1 3 0 8 に記憶している公開鍵証明証。

## 【0 3 2 7】

最後に仲介許諾証発行の履歴を表す新しいエントリを仲介許諾証発行履歴 D B 1 3 0 9 に追加して終了する。追加されるエントリの各属性には以下の値が格納される。

## 【0 3 2 8】

## 【表 3 3】

仲介許諾証識別子属性：1 7 0 3 で作成した識別子。

公開鍵識別子属性：仲介許諾証依頼に含まれる仲介許諾仕様の公開鍵識別子フィールドの値。

リテラ識別子属性：仲介許諾証依頼に含まれる仲介許諾仕様の被許諾者フィールドの値。

利用条件限定情報属性：1 7 0 5 で決定した利用条件限定情報の値。

有効期間開始属性：1 7 0 4 で決定した有効期間の開始日時。

有効期間終了属性：1 7 0 4 で決定した有効期間の終了日時。

発行日属性：1 7 0 5 で作成した仲介許諾証の発行日フィールドに記載した値。

## 【0 3 2 9】

## 【プロバイダが持つその他の機能】

本実施例のプロバイダは、仲介許諾証発行の履歴情報をリテラに送付することができる。

## 【0 3 3 0】

リテラに渡される仲介許諾証発行の履歴情報は、そのリテラに発行された仲介許諾証についての情報であり、仲介許諾証発行履歴作成部 1 3 1 0 で作成され、入出力制御部 1 3 0 1 を介してリテラに送付される。この履歴は、プロバイダがリテラに対して仲介許諾証発行の手数料を請求する場合の根拠となる。

## 【0 3 3 1】

仲介許諾証発行履歴作成部 1 3 1 0 は、履歴を作成するリテラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、仲介許諾証発行履歴 D B

1309から、リテラ識別子属性の値が指定されたリテラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その仲介許諾証識別子属性、公開鍵識別子属性、利用条件限定情報属性、有効期間開始属性、有効期間終了属性、発行日属性の値を取り出す。本実施例では、履歴を作成するリテラの識別子と履歴作成の対象期間の指定はプロバイダのオペレータから受けるが、インターネット経由でリテラから入力されるように構成してもよい。

#### 【0332】

上記の履歴情報の送付方法は、電子メールでもよいし、WWWベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

#### 【0333】

##### 〔リテラの構成〕

図18は、本実施例のリテラの構成図である。

#### 【0334】

本実施例のリテラは、仲介許諾証依頼を作成してインターネットを介してプロバイダに送付する機能、インターネットを介して入力される仲介許諾証送付、利用許可証依頼、利用許可証送付を処理する機能、利用許可証仲介の履歴を作成してインターネットを介してプロバイダや利用許可証仲介の依頼者に送付する機能を持つ。リテラは、入出力制御部1801、処理選択部1802、仲介許諾証依頼作成部1803、利用許可証依頼処理部1804、仲介許諾証送付処理部1805、利用許可証送付処理部1806、仲介許諾証DB1807、利用許可証仲介履歴DB1808、署名鍵記憶部1809、証明証記憶部1810、利用許可証仲介プロバイダ用履歴作成部1811、利用許可証仲介依頼者用履歴作成部1812から構成され、入出力制御部1801を介してインターネットに接続されている。

#### 【0335】

本実施例のリテラの各部の役割を以下に述べる。

#### 【0336】

入出力制御部1801：インターネットを介したデータの入力を監視するとともに、仲介許諾証依頼作成部1803、利用許可証依頼処理部1804、利用許可証送付処理部1806が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部1801への入力、あるいは、入出力制御部1804からインターネットへの出力の方法としては、入出力制御部1801と接続されたWWWサイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意しているWWWサイトにアクセスしてリテラが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部1801を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部1802：入力したデータが、利用許可証依頼、仲介許諾証送付、利用許可証送付のいずれであるかを判断し、利用許可証依頼であれば利用許可証依頼処理部1804を、仲介許諾証送付であれば仲介許諾証送付処理部1805を、利用許可証送付であれば利用許可証送付処理部1806を呼び出す。

仲介許諾証依頼作成部1803：仲介許諾証依頼を作成し、入出力制御部1801を介してプロバイダに送付する。仲介許諾証依頼作成の過程で、署名鍵記憶部1809と証明証記憶部1810にアクセスする。

利用許可証依頼処理部1804：消費者からの利用許可証依頼を処理し、第二の利用許可証依頼を作成して、入出力制御部1801を介してセンタに送付する。処理の過程で、仲介許諾証DB1807を参照するとともに、署名鍵記憶部1809と証明証記憶部1810にアクセスする。

仲介許諾証送付処理部1805：プロバイダからの仲介許諾証送付を処理し、該仲介許諾証送付に含まれている仲介許諾証を仲介許諾証DB1807に登録する。

利用許可証送付処理部1806：センタからの利用許可証送付を処理し、第二の利用許可証送付をを作成して、入出力制御部1801を介して利用許可証の依頼者に送付する。処理の過程で、利用許可証仲介履歴DB1808を更新するとともに、署名鍵記憶部1809と証明証記憶部1810にアクセスする。

仲介許諾証DB1807：プロバイダからこのリテラに対して発行された仲介許諾証に関する情報を保持するDB。

利用許可証仲介履歴DB1808：このリテーラが仲介した利用許可証についての履歴を保持するDB。

署名鍵記憶部1809：リテーラが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部1810：署名鍵記憶部1809に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

利用許可証仲介プロバイダ用履歴作成部1811：各プロバイダ毎の利用許可証仲介の履歴を作成し、入出力制御部1801を介してプロバイダに送付する。

利用許可証仲介依頼者用履歴作成部1812：リテーラが受け取った利用許可証仲介依頼の依頼者毎の利用許可証仲介の履歴を作成し、入出力制御部1801を介して依頼者に送付する。

#### 【0337】

〔リテーラが持つデータベース〕

リテーラは、仲介許諾証DB1807と利用許可証仲介履歴DB1808の2つのデータベースを持っている。

#### 【0338】

仲介許諾証DB1807は、リテーラが複数のプロバイダから受けた仲介許諾証に関する情報を保持したデータベースである。

#### 【0339】

仲介許諾証DB1807の構造を図19に示す。仲介許諾DB1807は以下の5つの属性からなるテーブルである。各エントリがそれぞれ一つの仲介許諾証にあたる。

#### 【0340】

##### 【表34】

仲介許諾証識別子属性：プロバイダから発行された仲介許諾証に割り当てられている仲介許諾証識別子。

公開鍵識別子属性：プロバイダから発行された仲介許諾証で利用許可証発行の仲介が許諾された検証用公開鍵の識別子。

プロバイダ識別子属性：仲介許諾証を発行したプロバイダの識別子。

仲介許諾証属性：プロバイダから発行された仲介許諾証自体を B E R にしたがってエンコードしたデータ。

プロバイダ証明証属性：仲介許諾証を発行したプロバイダのデジタル署名を検証できる公開鍵を含む公開鍵証明証を B E R にしたがってエンコードしたデータ。

#### 【 0 3 4 1 】

利用許可証仲介履歴 D B 1 8 0 8 は、リテーラが仲介した利用許可証に関する情報を保持したデータベースである。

#### 【 0 3 4 2 】

利用許可証仲介履歴 D B 1 8 0 8 の構造を図 2 0 に示す。利用許可証仲介履歴 D B 1 8 0 8 は以下の 8 つの属性からなるテーブルである。各エントリがそれぞれ一つの利用許可証の仲介にあたる。

#### 【 0 3 4 3 】

##### 【表 3 5】

利用許可証識別子属性：仲介した利用許可証にセンタが割り当てた識別子。

公開鍵識別子属性：仲介した利用許可証の正当性を検証できる検証用公開鍵にセンタが割り当てた識別子。

プロバイダ識別子属性：公開鍵識別子属性で指定された検証用公開鍵のユーザであるプロバイダの識別子。

消費者識別子属性：利用許可証の発行を受けた消費者の識別子。

依頼者識別子属性：利用許可証依頼をリテーラに送付してきたエンティティの識別子。

利用条件属性：仲介された利用許可証に記載された利用条件。

依頼日時属性：リテーラが受け取った利用許可証依頼の作成日時。

発信日時属性：リテーラが利用許可証送付を作成した日時。

#### 【 0 3 4 4 】

##### 【仲介許諾証依頼作成部】

本実施例のリテーラは、プロバイダが提供しているデジタルコンテンツの販売を始めたい場合、そのデジタルコンテンツに割りあてられた検証用公開鍵に対応する利用許可証の仲介を許諾する仲介許諾証をプロバイダから受けなければなら

ない。プロバイダから仲介許諾証を受け取るため、リテーラは仲介許諾証依頼作成部 1 8 0 3 において仲介許諾証依頼を作成し、入出力制御部 1 8 0 1 を介してプロバイダに送付する。

#### 【 0 3 4 5 】

仲介許諾証依頼作成部 1 8 0 3 では、仲介許諾証依頼の各フィールドに以下の値を設定する。

#### 【 0 3 4 6 】

##### 【表 3 6】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：仲介許諾証の依頼先であるプロバイダの識別子。

日時フィールド：現在の時刻。

仲介許諾仕様フィールド：作成してもらう仲介許諾証に対するリテーラからの希望を記載する。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、仲介許諾証依頼作成部 1 8 0 3 は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部 1 8 0 9 にアクセスして入手する。

証明証フィールド：証明証記憶部 1 8 1 0 に記憶している公開鍵証明証。

#### 【 0 3 4 7 】

仲介許諾証依頼の仲介許諾仕様フィールドに記載される仲介許諾仕様の各フィールドには以下の値が設定される。

#### 【 0 3 4 8 】

##### 【表 3 7】

許諾者フィールド：仲介許諾証を発行してほしいプロバイダの識別子。

被許諾者フィールド：自分自身すなわちリテーラの識別子。

公開鍵識別子フィールド：仲介許諾証を発行してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子。

希望利用条件限定情報フィールド：リテーラが仲介許諾証に記載してほしいと希

望する利用条件限定情報。

【0349】

〔仲介許諾証送付処理部〕

仲介許諾依頼作成部1803で仲介許諾証依頼が作成されプロバイダに送付されると、その返信としてプロバイダから仲介許諾証送付が送信されてくる。仲介許諾証送付は、入出力制御部1801および処理選択部1802を経由して仲介許諾証送付処理部1805に送られ、そこで処理される。

【0350】

図21は、本実施例のリテラが持つ仲介許諾証送付処理部1805の動作を示すフローチャートである。仲介許諾証送付処理部1805の動作を図21にしたがって説明する。

【0351】

まず、処理選択部1802から入力された仲介許諾証送付、および、該仲介許諾証送付に含まれる仲介許諾証のデジタル署名を検証する(2101)。検証鍵は仲介許諾証送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA108から公開鍵証明証を取得してから署名の検証を行う。署名の検証のために、仲介許諾証送付処理部1805はデジタル署名の検証を専門に行う署名検証部を含んでいる。

【0352】

2101で、デジタル署名の検証に失敗した場合、エラー処理を行った後(2104)、終了する。

【0353】

2101で、デジタル署名の検証に成功した場合、仲介許諾証送付に含まれている仲介許諾証の作成者が正しいプロバイダであるかどうかを確認される(2102)。正しいプロバイダであるかどうかの判断基準にはいくつかバリエーションが有り得る。たとえば、仲介許諾証送付に含まれている仲介許諾証の発行者フィールドの値が、自分が依頼した仲介許諾証依頼に含まれる仲介許諾仕様の許諾者フィールドに記載されている識別子と一致するという基準はその一例である。仲介許諾証送付に含まれている仲介許諾証で利用許可証の仲介が許諾される検証

用公開鍵と、該仲介許諾証の発行者との関係を確認したければ、センタが発行した検証用公開鍵情報を確認すればよい。検証用公開鍵情報は公開可能な情報であるので、センタあるいはプロバイダが検証用公開鍵情報を自由にダウンロードできる形で公開することが可能である。

#### 【0354】

2102の検査で、仲介許諾証の作成者が正しいプロバイダではなかった場合、エラー処理を行った後(2104)、終了する。

#### 【0355】

2102の検査で、仲介許諾証の作成者が正しいプロバイダと判断した場合、仲介許諾証DB1807に新しいエントリを追加する(2103)。新しいエントリの各属性には以下の値が設定される。

#### 【0356】

##### 【表38】

仲介許諾証識別子属性：仲介許諾証送付に含まれる仲介許諾証の仲介許諾証識別子フィールドの値。

公開鍵識別子属性：仲介許諾証送付に含まれる仲介許諾証の公開鍵識別子フィールドの値。

プロバイダ識別子属性：仲介許諾証送付に含まれる仲介許諾証の発行者フィールドの値。

仲介許諾証属性：仲介許諾証送付に含まれる仲介許諾証をBERにしたがってエンコードした結果。

プロバイダ証明証属性：仲介許諾証送付に含まれるプロバイダの署名の検証鍵を含む公開鍵証明証をBERにしたがってエンコードした結果。

#### 【0357】

##### 【利用許可証依頼処理部】

図22は、本実施例のリテーラが持つ利用許可証依頼処理部1804の内部構成を示した図である。

#### 【0358】

利用許可証依頼処理部1804は、消費者あるいは他のリテーラから送信され



た利用許可証依頼を処理し、センタへの利用許可証依頼を作成し、入出力制御部 1801 経由でセンタへ送付する機能を持ち、処理制御部 2201、署名検証部 2202、エラーメッセージ作成部 2203、利用許可証依頼作成部 2204、署名作成部 2205、利用条件作成部 2206 から構成される。

#### 【0359】

利用許可証依頼処理部 1804 を構成する各部の役割を以下に述べる。

#### 【0360】

処理制御部 2201：処理選択部 1802 からの入力、入出力制御部 1801 への出力、仲介許諾証 DB 1807 の参照、利用許可証仲介履歴 DB 1808 へのエントリの追加の機能を担うとともに、利用許可証依頼の処理全体を制御する。

署名検証部 2202：処理選択部 1802 から入力される利用許可証依頼のデジタル署名を検証する。

エラーメッセージ作成部 2203：エラーメッセージを作成する。

利用許可証依頼作成部 2204：センタへ送付する利用許可証依頼を作成する。

利用許可証依頼にデジタル署名を添付するために署名作成部 2205 を呼び出す。さらに、リテーラの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 1810 にアクセスする。

署名作成部 2205：利用許可証依頼作成部 2204 で作成する利用許可証依頼のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 1809 にアクセスする。

利用条件作成部 2206：依頼する利用許可証に含まれるべき利用条件を作成する。

#### 【0361】

図 23 は、本実施例のリテーラが持つ利用許可証依頼処理部 1804 の処理制御部 2201 の動作を示すフローチャートである。処理制御部 2201 の動作を図 23 にしたがって説明する。

#### 【0362】

まず、処理選択部 1802 から入力された利用許可証依頼のデジタル署名を検証する（2301）。検証鍵は該利用許可証依頼の証明証フィールドに添付され

ているものを使用するが、必要な公開鍵証明書が証明書フィールドに存在しない場合には、CA108から公開鍵証明書を取得してから署名の検証を行う。

#### 【0363】

署名の検証に失敗した場合、エラーメッセージ作成部2203でエラーメッセージを作成して入出力制御部1801に出力した後(2307)、終了する。

#### 【0364】

署名の検証に成功した場合、入力された利用許可証依頼で利用許可証の仲介を依頼されている検証用公開鍵の仲介が許諾されているかどうかを検査する(2302)。仲介許諾証DB1807に、利用許可証依頼で依頼された検証用公開鍵に対する仲介許諾証が存在し、かつ、利用許可証依頼に記載されている利用条件が、仲介許諾証DB1807に保持されている仲介許諾証に記載されている利用条件限定情報の範囲内である場合に許諾されていると判断する。

#### 【0365】

2302の検査で仲介が許諾されていないと判断された場合、エラーメッセージ作成部2203でエラーメッセージを作成して入出力制御部1801に出力した後(2307)、終了する。

#### 【0366】

2302の検査で仲介が許諾されていると判断された場合、利用許可証依頼を受け付けるかどうかを判断する(2303)。入力された利用許可証依頼の発信者である消費者やリテラが信用できない場合は、ここで利用許可証依頼を受け付けないことを決定する。

#### 【0367】

2303で利用許可証依頼を受け付けないと判断した場合、エラーメッセージ作成部2203でエラーメッセージを作成して入出力制御部1801に出力した後(2307)、終了する。

#### 【0368】

2303で利用許可証依頼を受け付けると判断した場合、利用条件作成部2206を呼び出し、センタへ送付する利用許可証依頼に記載する利用条件を作成させ、その結果を受けとる(2304)。利用条件作成部2206が作成する利用

条件は、入力された利用許可証依頼に記載されている利用条件のままでもよいし、必要ならリテラの裁量で適切なものに修正してもよい。

#### 【0369】

利用条件が決まったら、処理中の利用許可証依頼に関する情報を保持したエントリを利用許可証仲介履歴DB1808に追加する(2305)。新しいエントリの各属性には以下の値が設定される。

#### 【0370】

##### 【表39】

利用許可証識別子属性：この時点では値は設定されない。

公開鍵識別子属性：入力された利用許可証依頼に含まれる許可仕様の公開鍵識別子フィールドに記載されている値。

プロバイダ識別子属性：公開鍵識別子属性に設定された識別子で特定される検証用公開鍵情報のユーザであるプロバイダの識別子。該プロバイダの識別子は、仲介許諾証DBを参照して得ることができる。すなわち、本DBの公開鍵識別子属性に設定された識別子を仲介許諾証DBの公開鍵識別子属性の値に持つ仲介許諾証DBのエントリのプロバイダ識別子属性がそれにあたる。

消費者識別子属性：入力された利用許可証依頼に含まれる許可仕様の消費者識別子フィールドの値。

依頼者識別子属性：入力された利用許可証依頼の発信者フィールドの値。

利用条件属性：2304で決定した利用条件。

依頼日時属性：入力された利用許可証依頼の日時フィールドの値。

発信日時属性：この時点では値は設定されない。

#### 【0371】

最後にセンタへ送付する利用許可証依頼を作成し、入出力制御部1801を介してセンタに送付し(2306)、終了する。センタへ送付する利用許可証依頼の各フィールドには以下の値が設定される。

#### 【0372】

##### 【表40】

発信者フィールド：自分自身すなわちリテラの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の日時。

許可内容フィールド：後述する許可仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部 2 2 0 5 を呼び出して署名値を作成させ、結果をこのフィールドに設定する。署名鍵は署名鍵記憶部 1 8 0 9 にアクセスして入手する。

証明証フィールド：証明証記憶部 1 8 1 0 に記憶している公開鍵証明証。

### 【 0 3 7 3 】

許可内容フィールドに記載される許可仕様の各フィールドには、以下の値が記載される。

### 【 0 3 7 4 】

#### 【表 4 1】

公開鍵識別子フィールド：入力された利用許可証依頼に含まれる許可仕様に記載された公開鍵識別子フィールドの値。

消費者識別子フィールド：入力された利用許可証依頼に含まれる許可仕様に記載された消費者識別子フィールドの値。

利用条件フィールド：2 3 0 4 で決定した利用条件。

仲介許諾フィールド：仲介許諾証 D B 1 8 0 7 に保持されている、利用許可証依頼で依頼された検証用公開鍵に対する仲介許諾証。

### 【 0 3 7 5 】

#### 〔利用許可証送付処理部〕

図 2 4 は、本実施例のリテーラが持つ利用許可証送付処理部 1 8 0 6 の内部構成を示した図である。

### 【 0 3 7 6 】

利用許可証送付処理部 1 8 0 6 は、センタあるいは他のリテーラからの送信された利用許可証送付を処理し、利用許可証の依頼者に送付する利用許可証送付を作成し、入出力制御部 1 8 0 1 経由で該依頼者に送付する機能を持ち、処理制御部 2 4 0 1、署名検証部 2 4 0 2、エラーメッセージ作成部 2 4 0 3、利用許可

証送付作成部 2404、署名作成部 2405 から構成される。

【0377】

利用許可証送付処理部 1806 を構成する各部の役割を以下に述べる。

【0378】

処理制御部 2401：処理選択部 1802 からの入力、入出力制御部 1801 への出力、利用許可証仲介履歴 DB 1808 のエントリ更新の機能を担うとともに、利用許可証送付の処理全体を制御する。

署名検証部 2402：処理選択部 1802 から入力される利用許可証送付、および利用許可証送付に含まれる利用許可証のデジタル署名を検証する。

エラーメッセージ作成部 2403：エラーメッセージを作成する。

利用許可証送付作成部 2404：利用許可証の依頼者に送付する利用許可証送付を作成する。新たに作成する利用許可証送付にデジタル署名を添付するために署名作成部 2405 を呼び出す。さらに、リテララの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 1810 にアクセスする。

署名作成部 2405：利用許可証送付作成部 2404 で作成する利用許可証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 1809 にアクセスする。

【0379】

図 25 は、本実施例のリテララが持つ利用許可証送付処理部 1806 の処理制御部 2401 の動作を示すフローチャートである。処理制御部 2401 の動作を図 25 にしたがって説明する。

【0380】

まず、処理選択部 1802 から入力された利用許可証送付および該利用許可証送付に含まれる利用許可証のデジタル署名を検証する（2501）。検証鍵は該利用許可証送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA108 から公開鍵証明証を取得してから署名の検証を行う。

【0381】

署名の検証に失敗した場合、エラーメッセージ作成部 2403 でエラーメッセ

ージを作成して入出力制御部1801に出力した後(2504)、終了する。

【0382】

署名の検証に成功した場合、入力された利用許可証送付で送付された内容にしたがって、利用許可証仲介履歴DB1808のエントリを更新する(2502)。更新されるエントリは、入力された利用許可証送付に対応する利用許可証依頼を処理した時に追加されたエントリであり、エントリの公開鍵識別子属性、消費者識別子属性の値が、それぞれ入力された利用許可証送付に含まれる利用許可証の公開鍵識別子フィールド、受領者フィールドの値と一致し、該エントリの利用許可証識別子属性と発信日時属性の値が設定されていないものである。

【0383】

更新対象のエントリの各属性は以下のように更新される。

【0384】

【表42】

利用許可証識別子属性：入力された利用許可証送付に含まれる利用許可証の利用許可証識別子フィールドの値。

公開鍵識別子属性：変化なし。

プロバイダ識別子属性：変化なし。

消費者識別子属性：変化なし。

依頼者識別子属性：変化なし。

利用条件属性：入力された利用許可証送付に含まれる利用許可証の利用条件フィールドの値。

依頼日時属性：変化なし。

発信日時属性：現在の時刻。

【0385】

最後に、利用許可証の依頼者に送付する新たな利用許可証送付を作成し、入出力制御部1801を介して利用許可証の依頼者に送付し(2503)、終了する。新たに作成される利用許可証送付の各フィールドには以下の値が設定される。

【0386】

【表43】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：2502で更新された利用許可証仲介履歴DB1808のエントリの依頼者識別子属性の値。

日時フィールド：2502で更新された利用許可証仲介履歴DB1808のエントリの発信日時属性の値。

利用許可証フィールド：入力された利用許可証送付に含まれる利用許可証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部2405を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部1810に記憶している公開鍵証明証と、入力された利用許可証送付の証明証フィールドに含まれる証明証のうち、該利用許可証送付に含まれる利用許可証のデジタル署名を検証できる検証鍵を含む公開鍵証明証。

#### 【0387】

##### 〔利用許可証依頼処理の課金・決済〕

本実施例のリテーラは、利用許可証依頼の処理の過程で利用許可証発行料金の課金あるいは決済を行うことができる。課金あるいは決済の処理は、消費者からの利用許可証依頼をうけた後、センタに利用許可証依頼を送付する前に行われる。

#### 【0388】

課金の場合は、利用許可証依頼の処理の過程で、消費者毎に利用許可証発行料金を加算しておき、後に消費者に対して請求する。そのため、本実施例のリテーラは、消費者毎に現在の利用許可証発行料金高を保持するデータベースをもっている。

#### 【0389】

本実施例のリテーラは、利用許可証依頼の処理のたび毎に利用許可証発行料金の決済を行うこともできる。決済の方法としては、消費者が所持するクレジットカードによる決済や、プリペイドの方式等種々のものが利用可能であるが、いずれも、消費者からの利用許可証依頼をうけた後、決済が終了した事が確認されて

から、センタに利用許可証依頼を送付する。

【0390】

[リテラが発行する履歴情報]

本実施例のリテラは利用許可証仲介の履歴情報をプロバイダに送付することができる。

【0391】

プロバイダに渡される利用許可証仲介の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する利用許可証の仲介についての情報であり、利用許可証仲介プロバイダ用履歴作成部1811で作成され、入出力制御部1801を介してプロバイダに送付される。この履歴は、リテラがプロバイダに送付するマージンの額に対する根拠となる。

【0392】

利用許可証仲介プロバイダ用履歴作成部1811は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証仲介履歴DB1808から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その利用許可証識別子属性、公開鍵識別子属性、利用条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はリテラのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【0393】

また、本実施例のリテラは利用許可証仲介の履歴情報を利用許可証仲介の依頼者にも送付することができる。

【0394】

依頼者に渡される利用許可証仲介の履歴情報は、その依頼者から依頼された利用許可証の仲介についての情報であり、利用許可証仲介依頼者用履歴作成部1812で作成され、入出力制御部1801を介して依頼者に送付される。この履歴は、リテラが依頼者に対して手数料の請求を行う場合の根拠となる。



## 【 0 3 9 5 】

利用許可証仲介依頼者用履歴作成部 1 8 1 2 は、履歴を作成する依頼者の識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証仲介履歴 DB 1 8 0 8 から、依頼者識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その利用許可証識別子属性、公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、利用条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作成する依頼者の識別子と履歴作成の対象期間の指定はリテーラのオペレータから受けるが、インターネット経由で依頼者から入力されるように構成してもよい。

## 【 0 3 9 6 】

上記の履歴情報のプロバイダや依頼者への送付方法は、電子メールでもよいし、WWWベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

## 【 0 3 9 7 】

## 〔消費者端末の構成〕

図 2 6 は、本実施例の消費者端末の構成図である。

## 【 0 3 9 8 】

本実施例の消費者は、消費者識別子と消費者秘密情報を内蔵した携帯型記憶装置を所持しており、インターネットを介してリテーラから利用許可証を受け取って該携帯型記憶装置に記憶する。消費者端末は、入出力制御部 2 6 0 2、利用許可証依頼作成部 2 6 0 3、利用許可証送付処理部 2 6 0 4、署名鍵記憶部 2 6 0 5、証明証記憶部 2 6 0 6、携帯型記憶装置制御部 2 6 0 7 から構成され、入出力制御部 2 6 0 2 を介してインターネットに接続されるとともに、携帯型記憶装置制御部 2 6 0 7 を介して携帯型記憶装置と接続されている。

## 【 0 3 9 9 】

本実施例の消費者端末の各部の役割を以下に述べる。

## 【 0 4 0 0 】

入出力制御部 2 6 0 2 : インターネットを介したデータの入力を受け付けるとと

もに、利用許可証依頼作成部 2 6 0 3 が作成した利用許可証依頼をインターネットを介して出力する。インターネットからの入出力制御部 2 6 0 2 への入力、あるいは、入出力制御部 2 6 0 2 からインターネットへの出力の方法としては、他のエンティティが用意している WWW サイトにアクセスして消費者端末が作成したデータを送るもの、あるいは電子メールシステムと入出力制御部 2 6 0 2 を自動的にあるいは人手によって連動させるものなどが使用できる。

#### 【 0 4 0 1 】

利用許可証依頼作成部 2 6 0 3 : 利用許可証依頼を作成し、入出力制御部 2 6 0 2 を介してリテーラに送付する。利用許可証依頼の作成の過程で、署名鍵記憶部 2 6 0 5 と証明証記憶部 2 6 0 6 にアクセスするとともに、携帯型記憶装置制御部 2 6 0 7 を介して携帯型記憶装置 2 6 0 8 にアクセスする。

利用許可証送付処理部 2 6 0 4 : リテーラからの利用許可証送付を処理し、該利用許可証送付に含まれている利用許可証を携帯型記憶装置制御部 2 6 0 7 を介して携帯型記憶装置 2 6 0 8 に記録する。

署名鍵記憶部 2 6 0 5 : 消費者端末が作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部 2 6 0 6 : 署名鍵記憶部 2 6 0 5 に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

携帯型記憶装置制御部 2 6 0 7 : 携帯型記憶装置 2 6 0 8 へのデータの書込みとアクセスを行う。

#### 【 0 4 0 2 】

本実施例では、利用許可証依頼にデジタル署名を施す場合に使用する署名鍵や、その署名鍵で作成した署名を検証する検証鍵を含む公開鍵証明証は、消費者端末が保持しているものとしたが、これらが携帯型記憶装置に保持されているように構成してもよい。

#### 【 0 4 0 3 】

本実施例では、消費者が携帯型記憶装置を所持しており、該記憶装置に利用許可証を記憶するように構成しているが、もちろん、消費者端末自体の記憶領域に記憶するように構成してもよい。

## 【0404】

## [利用許可証依頼作成部]

本実施例の消費者端末は、該端末を利用している消費者が利用したいデジタルコンテンツがある場合、そのデジタルコンテンツの利用許可証の仲介を依頼する利用許可証依頼を利用許可証依頼作成部2603で作成し、入出力制御部2602を介してリテーラに送付する。

## 【0405】

利用許可証依頼作成部2603では、利用許可証依頼の各フィールドに以下の値を設定する。

## 【0406】

## 【表44】

発信者フィールド：自分自身すなわち消費者端末の識別子。

受信者フィールド：リテーラの識別子。

日時フィールド：現在の時刻。

許可内容フィールド：後述する許可仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、利用許可証依頼作成部2603は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部2605にアクセスして入手する。

証明証フィールド：証明証記憶部2606に記憶している公開鍵証明証。

## 【0407】

許可内容フィールドに指定される許可仕様の各フィールドには以下の値が設定される。

## 【0408】

## 【表45】

公開鍵識別子フィールド：利用したいデジタルコンテンツに割り当てられている検証用公開鍵の識別子。

消費者識別子フィールド：消費者端末を使用している消費者の識別子。消費者識

別子は携帯型記憶装置 2608 に記憶されており、利用許可証依頼作成部 2603 は、携帯型記憶装置制御部 2607 を介して携帯型記憶装置 2608 から消費者識別子を入力する。

利用条件フィールド：消費者の希望等を反映した適切なものを利用許可証依頼作成部 2603 が決定して設定。

仲介許諾証フィールド：設定しない。

#### 【0409】

##### [利用許可証送付処理部]

利用許可証依頼作成部 2603 で利用許可証依頼が作成されリテラに送付されると、その返信としてリテラから利用許可証送付が送信されてくる。利用許可証送付は、入出力制御部 2602 を経由して利用許可証送付処理部 2604 に入力され、そこで処理される。

#### 【0410】

図 27 は、本実施例の消費者端末が持つ利用許可証依頼作成部 2603 の動作を示すフローチャートである。利用許可証依頼作成部 2603 の動作を図 27 にしたがって説明する。

#### 【0411】

まず、入力された利用許可証送付および該利用許可証送付に含まれる利用許可証のデジタル署名を検証する (2701)。検証鍵は検証用公開鍵情報送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA108 から公開鍵証明証を取得してから署名の検証を行う。

#### 【0412】

2701 で、デジタル署名の検証に失敗した場合、エラー処理を行った後 (2704)、終了する。

#### 【0413】

2701 で、デジタル署名の検証に成功した場合、入力された利用許可証送付に含まれる利用許可証が、現在消費者端末を使用している消費者向けのものかどうかを検査される (2702)。検査は、携帯型記憶装置制御部 2607 を介し

て携帯型記憶装置 2 6 0 8 から入手した消費者識別子と、入力された利用許可証送付に含まれる利用許可証の受領者フィールドの値が一致するかどうかで行われる。

【0 4 1 4】

2 7 0 2 の検査で、入力された利用許可証送付に含まれる利用許可証が現在消費者端末を使用している消費者向けのものでないと判断された場合、エラー処理を行った後（2 7 0 4）、終了する。

【0 4 1 5】

2 7 0 2 の検査で、入力された利用許可証送付に含まれる利用許可証が現在消費者端末を使用している消費者向けのものであると判断された場合、該利用許可証を携帯型記憶装置制御部 2 6 0 7 を介して携帯型記憶装置 2 6 0 8 に記録し（2 7 0 3）、終了する。

本実施例では、消費者が携帯型記憶装置を所持し、そこに消費者識別子が記憶されているが、これが消費者端末中の記憶領域に記憶されるよう構成してもよい。

【0 4 1 6】

【発明の効果】

以上説明したように、この発明によれば、デジタルコンテンツ提供者が利用証明証を発行するファシリティの構築や維持管理からデジタルコンテンツ提供者が開放される。

【図面の簡単な説明】

【図 1】 本発明を適用した実施例の構成図である。

【図 2】 本発明を適用したセンタの構成図である。

【図 3】 本発明を適用したセンタの動作を示すフローチャートである。

【図 4】 本発明を適用したセンタが持つ検証用公開鍵情報依頼処理部の内部構成を示した図である。

【図 5】 本発明を適用したセンタが持つ検証用公開鍵情報依頼処理部の処理制御部の動作を示すフローチャートである。

【図 6】 本発明を適用したセンタが持つプロバイダ DB の構造を示した図で

ある。

【図 7】本発明を適用したセンタが持つ公開鍵ペア DB の構造を示した図である。

【図 8】本発明を適用したセンタが持つリテラ DB の構造を示した図である。

【図 9】本発明を適用したセンタが持つ消費者 DB の構造を示した図である。

【図 10】本発明を適用したセンタが持つ利用許可証発行履歴 DB の構造を示した図である。

【図 11】本発明を適用したセンタが持つ利用許可証依頼処理部の内部構成を示した図である。

【図 12】本発明を適用したセンタが持つ利用許可証依頼処理部の処理制御部の動作を示すフローチャートである。

【図 13】本発明を適用したプロバイダの構成図である。

【図 14】本発明を適用したプロバイダが持つ検証用公開鍵 DB の構造を示した図である。

【図 15】本発明を適用したプロバイダが持つ検証用公開鍵情報送付処理部の動作を示すフローチャートである。

【図 16】本発明を適用したプロバイダが持つ仲介許諾証依頼処理部の内部構成を示した図である。

【図 17】本発明を適用したプロバイダが持つ仲介許諾証依頼処理部の処理制御部の動作を示すフローチャートである。

【図 18】本発明を適用したリテラの構成図である。

【図 19】本発明を適用したリテラが持つ仲介許諾証 DB の構造を示した図である。

【図 20】本発明を適用したリテラが持つ利用許可証仲介履歴 DB の構造を示した図である。

【図 21】本発明を適用したリテラが持つ仲介許諾証送付処理部の動作を示すフローチャートである。

【図 2 2】本発明を適用したリテーラが持つ利用許可証依頼処理部の内部構成を示した図である。

【図 2 3】本発明を適用したリテーラが持つ利用許可証依頼処理部の処理制御部の動作を示すフローチャートである。

【図 2 4】本発明を適用したリテーラが持つ利用許可証送付処理部の内部構成を示した図である。

【図 2 5】本発明を適用したリテーラが持つ利用許可証送付処理部の処理制御部の動作を示すフローチャートである。

【図 2 6】本発明を適用した消費者端末の構成図である。

【図 2 7】本発明を適用した消費者端末が持つ利用許可証依頼作成部の動作を示すフローチャートである。

【図 2 8】本発明を適用した携帯型記憶装置と利用許可証検査機能付きソフトウェアの内部構成例を示した図である。

【図 2 9】利用許可証の検証の際の携帯型記憶装置と利用許可証検証機能付きソフトウェア動作を示すフローチャートである。

【図 3 0】本発明を適用した利用許可証検査機能付きコンテンツプロセッシングソフトウェアと利用許可証明部の内部構成例を示した図である。

【図 3 1】利用許可証の検証の際の利用許可証検査機能付きコンテンツプロセッシングソフトウェアと利用許可証明部の動作を示すフローチャートである。

【図 3 2】本発明を適用した利用許可証検査機能付きコンテンツ復号ソフトウェアと利用許可証明部の内部構成例を示した図である。

【図 3 3】利用許可証の検証の際の利用許可証検査機能付きコンテンツ復号ソフトウェアと利用許可証明部の動作を示すフローチャートである。

【図 3 4】本発明を適用したプロバイダが持つ仲介許諾証発行履歴 DB の構造を示した図である。

【図 3 5】本発明を適用した利用許可証検査機能付きソフトウェアの構成例を示した図である。

【図 3 6】本発明を適用した利用許可証検査機能付きコンテンツプロセッシングソフトウェアの構成例を示した図である。

【図 3 7】 本発明を適用した利用許可証検査機能付きコンテンツプロセッシングソフトウェアで操作されるデジタルコンテンツのデータ構造を示した図である。

【図 3 8】 本発明を適用した利用許可証検査機能付きコンテンツ復号ソフトウェアの構成例を示した図である。

【図 3 9】 発明を適用した利用許可証検査機能付きコンテンツ復号ソフトウェアで復号されるデジタルコンテンツのデータ構造を示した図である。

【符号の説明】

- 1 0 1     インターネット 1 0 1
- 1 0 3、1 0 4     リテーラ
- 1 0 2     利用許可証発行センタ
- 1 0 5、1 0 6     プロバイダ
- 1 0 7     消費者端末
- 1 0 8     認証局 (C e r t i f i c a t e   A u t h o r i t y)
- 2 0 1     入出力制御部
- 2 0 2     処理選択部
- 2 0 3     検証用公開鍵情報依頼処理部
- 2 0 4     利用許可証依頼処理部
- 2 0 5     プロバイダ D B
- 2 0 6     公開鍵ペア D B
- 2 0 7     リテーラ D B
- 2 0 8     消費者 D B
- 2 0 9     利用許可証発行履歴 D B
- 2 1 0     署名鍵記憶部
- 2 1 1     証明証記憶部
- 2 1 2     利用許可証発行プロバイダ用履歴作成部
- 2 1 3     利用許可証発行リテーラ用履歴作成部
- 2 1 4     検証用公開鍵情報発行履歴作成部
- 4 0 1     処理制御部



- 4 0 2 署名検証部
- 4 0 3 公開鍵ペア作成部
- 4 0 4 公開鍵ペア識別子作成部
- 4 0 5 検証用公開鍵情報作成部
- 4 0 6 検証用公開鍵情報送付作成部
- 4 0 7 エラーメッセージ作成部
- 4 0 8 署名作成部
- 1 1 0 1 処理制御部
- 1 1 0 2 署名検証部
- 1 1 0 3 仲介許諾内容確認部
- 1 1 0 4 利用許可証識別子作成部
- 1 1 0 5 利用許可証作成部
- 1 1 0 6 利用許可証送付作成部
- 1 1 0 7 エラーメッセージ作成部
- 1 1 0 8 署名作成部
- 1 1 0 9 証明値作成部
- 1 1 1 0 利用条件作成部
- 1 3 0 1 入出力制御部
- 1 3 0 2 処理選択部
- 1 3 0 3 検証用公開鍵情報依頼作成部
- 1 3 0 4 検証用公開鍵情報送付処理部
- 1 3 0 5 仲介許諾証依頼処理部
- 1 3 0 6 検証用公開鍵 D B
- 1 3 0 7 署名鍵記憶部
- 1 3 0 8 証明証記憶部
- 1 3 0 9 仲介許諾証発行履歴 D B
- 1 3 1 0 仲介許諾証発行履歴作成部
- 1 8 0 1 入出力制御部
- 1 8 0 2 処理選択部

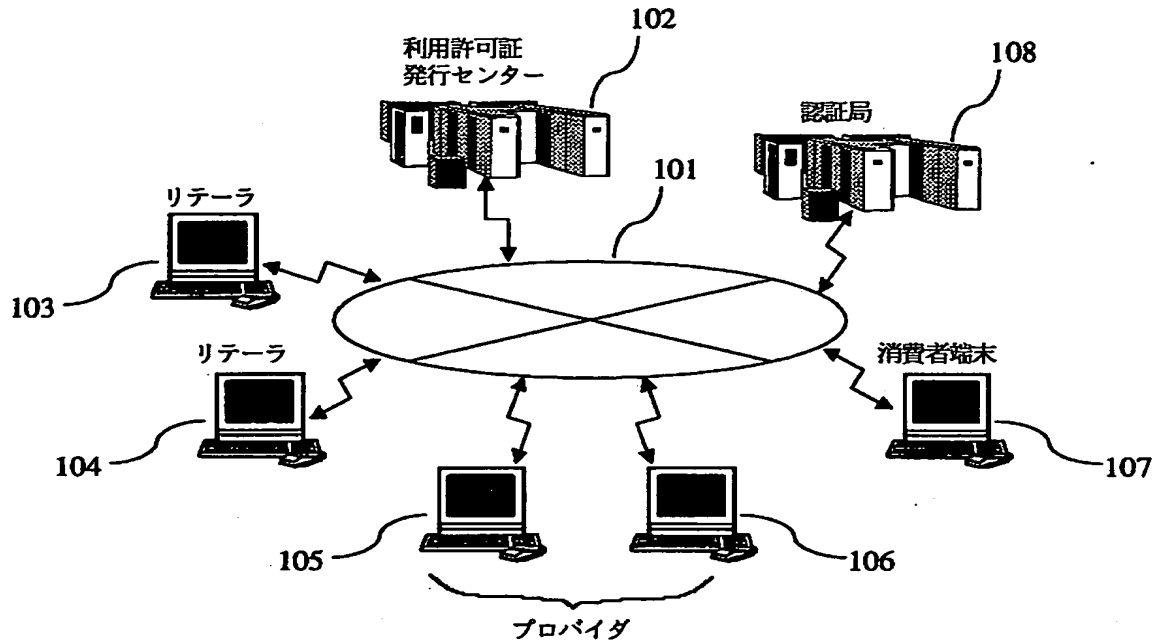
|         |                    |
|---------|--------------------|
| 1 8 0 3 | 仲介許諾証依頼作成部         |
| 1 8 0 4 | 利用許可証依頼処理部         |
| 1 8 0 5 | 仲介許諾証送付処理部         |
| 1 8 0 6 | 利用許可証送付処理部         |
| 1 8 0 7 | 仲介許諾証 D B          |
| 1 8 0 8 | 利用許可証仲介履歴 D B      |
| 1 8 0 9 | 署名鍵記憶部             |
| 1 8 1 0 | 証明証記憶部             |
| 1 8 1 1 | 利用許可証仲介プロバイダ用履歴作成部 |
| 1 8 1 2 | 利用許可証仲介依頼者用履歴作成部   |
| 2 6 0 2 | 入出力制御部             |
| 2 6 0 3 | 利用許可証依頼作成部         |
| 2 6 0 4 | 利用許可証送付処理部         |
| 2 6 0 5 | 署名鍵記憶部             |
| 2 6 0 6 | 証明証記憶部             |
| 2 6 0 7 | 携帯型記憶装置制御部         |
| 2 8 0 1 | 条件判定対象情報生成部        |
| 2 8 0 2 | チャレンジ生成部           |
| 2 8 0 3 | 公開鍵情報記憶部           |
| 2 8 0 4 | レスポンス検査部           |
| 2 8 1 1 | 入出力制御部             |
| 2 8 1 2 | 消費者秘密情報記憶部         |
| 2 8 1 3 | レスポンス計算部           |
| 2 8 1 4 | 利用条件判定部            |
| 2 8 1 5 | 利用許可証記憶部           |
| 3 0 0 1 | 入出力インタフェース         |
| 3 0 0 2 | チャレンジ生成部           |
| 3 0 0 3 | 条件判定対象情報生成部        |
| 3 0 0 4 | 公開鍵情報記憶部           |

|         |                        |
|---------|------------------------|
| 3 0 0 5 | レスポンス検査部               |
| 3 0 0 6 | 利用条件判定部                |
| 3 0 0 7 | 利用許可証記憶部               |
| 3 0 0 8 | 通信制御部                  |
| 3 0 1 1 | 入出力制御部                 |
| 3 0 1 2 | 消費者秘密情報記憶部             |
| 3 0 1 3 | レスポンス計算部               |
| 3 0 1 4 | 利用許可証記憶部               |
| 3 5 0 1 | 利用対象のソフトウェア            |
| 3 5 0 2 | 入出力制御部                 |
| 3 5 0 3 | 処理制御部                  |
| 3 5 0 4 | 第 1 の機能の実行部            |
| 3 5 0 5 | 第 2 の機能の実行部            |
| 3 5 0 6 | 第 1 の利用許可証検査部          |
| 3 5 0 7 | 第 2 の利用許可証検査部          |
| 3 5 0 8 | 携帯型記憶装置制御部             |
| 3 5 1 1 | 携帯型記憶装置                |
| 3 6 0 1 | デジタルコンテンツプロセッシングソフトウェア |
| 3 6 0 2 | 入出力制御部                 |
| 3 6 0 3 | 処理制御部                  |
| 3 6 0 4 | 表示実行部                  |
| 3 6 0 5 | 編集実行部                  |
| 3 6 0 6 | 印刷実行部                  |
| 3 6 0 7 | コンテンツデータ記憶部            |
| 3 6 0 8 | 利用許可証検査部               |
| 3 6 1 1 | 利用許可証明部                |

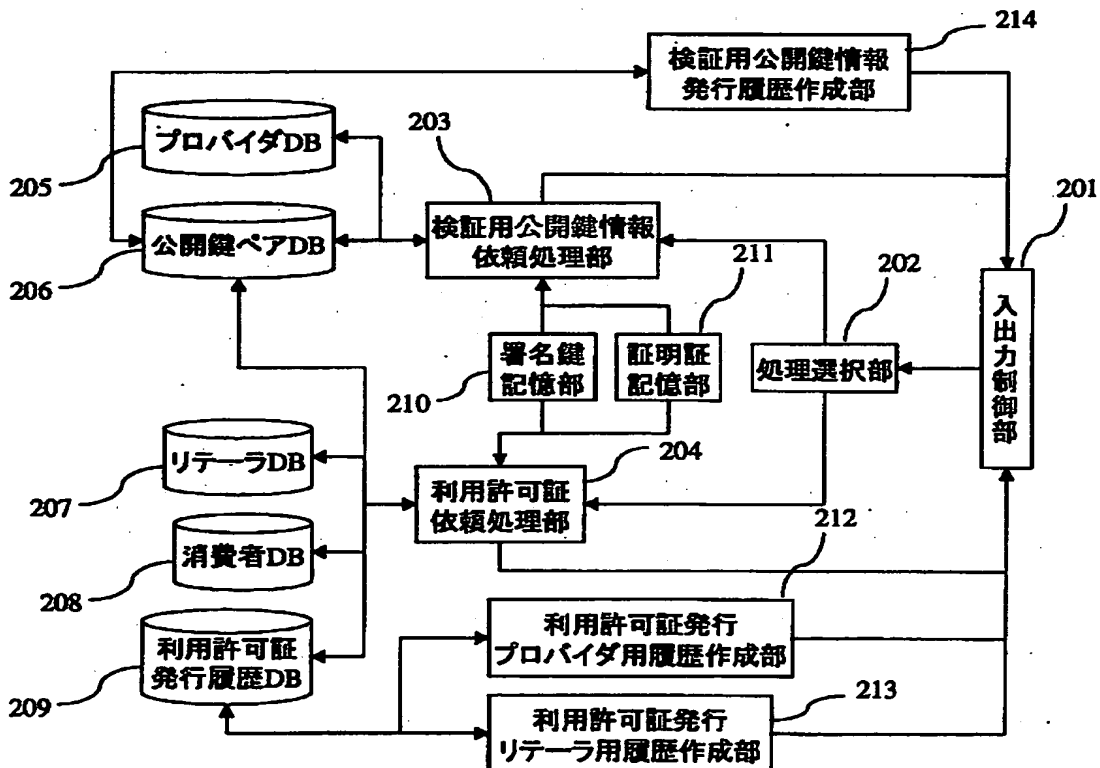
【書類名】

図面

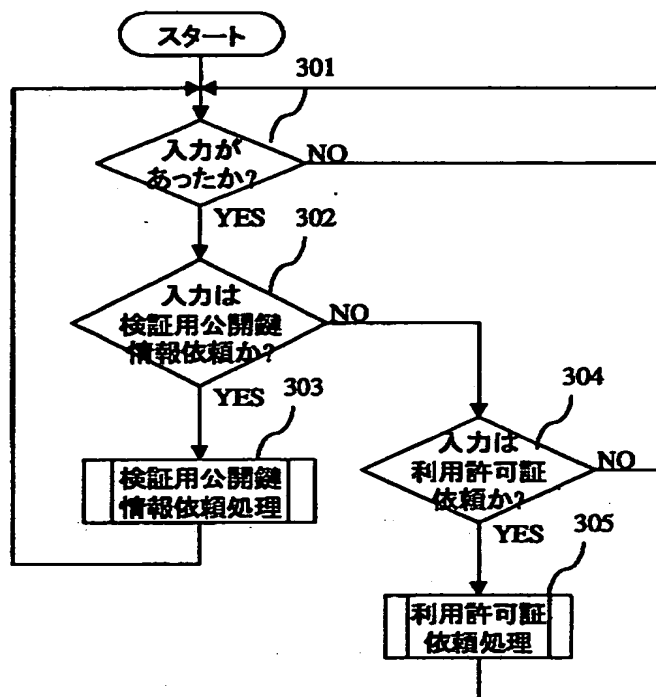
【図 1】



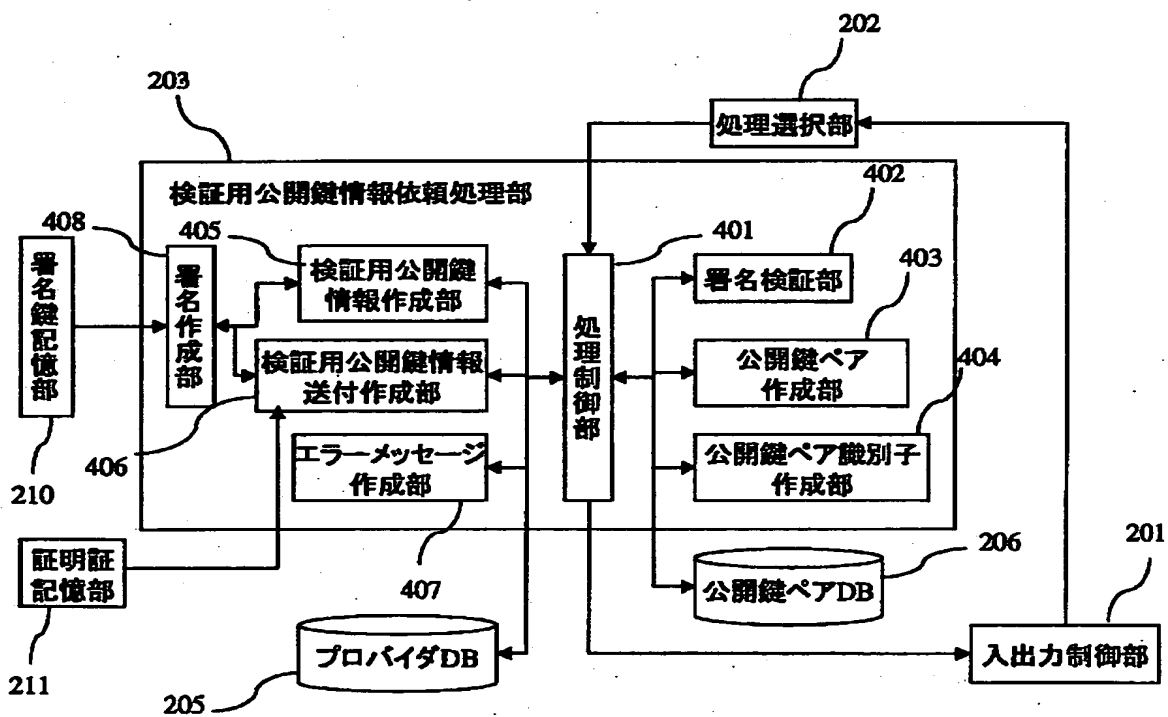
【図 2】



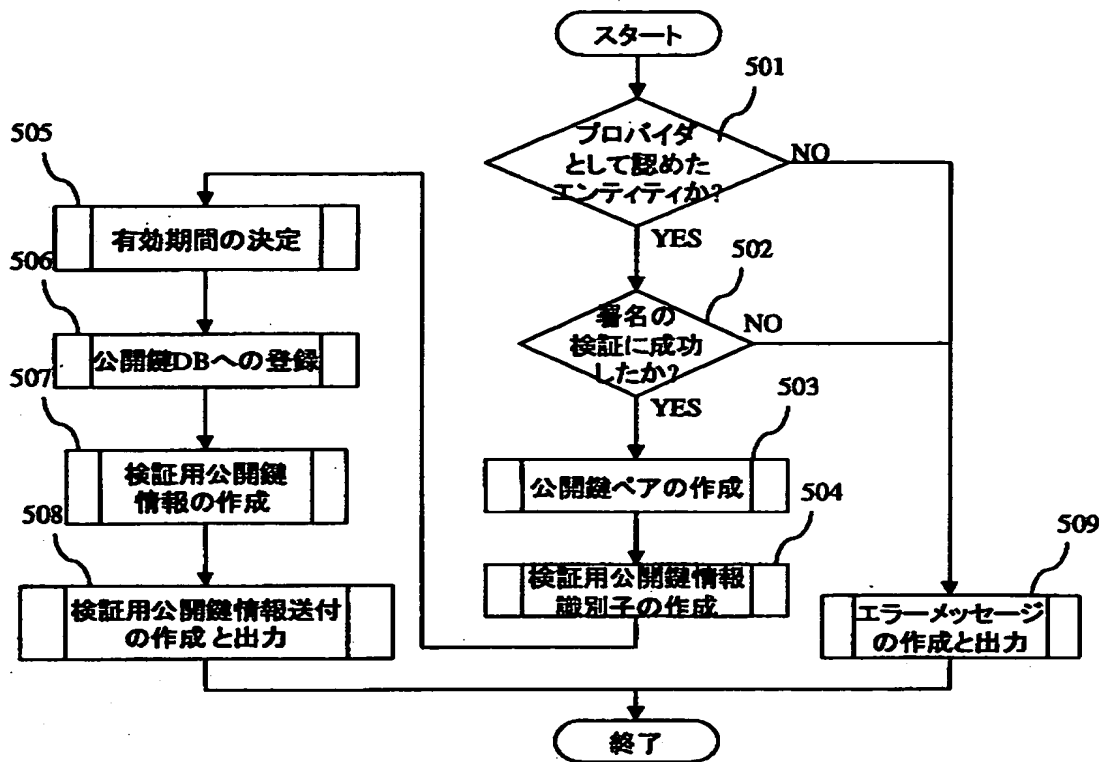
【図 3】



【図 4】



【図 5】



【図 6】

| プロバイダ識別子 |
|----------|
| PRV10001 |
| PRV10002 |
| PRV10003 |
| ...      |

【図 7】

| 公開鍵識別子  | 法数       | 公開鍵      | 秘密鍵      | プロバイダ識別子 | 有効期間開始    | 有効期間終了   | 発行日       |
|---------|----------|----------|----------|----------|-----------|----------|-----------|
| PK00001 | 10110... | 11001... | 10101... | PRV10001 | 2000.1.1  | 2001.1.1 | 2000.12.1 |
| PK00002 | 10010... | 11110... | 11011... | PRV10003 | 1999.3.5  | 2000.2.3 | 2000.1.2  |
| PK00003 | 11111... | 10000... | 10101... | PRV10001 | 1999.11.1 | 2000.5.1 | 2000.3.1  |
| ...     | ...      | ...      | ...      | ...      | ...       | ...      | ...       |

【図 8】

| リテラ識別子   |
|----------|
| RTL10001 |
| RTL10002 |
| RTL10003 |
| ...      |

【図 9】

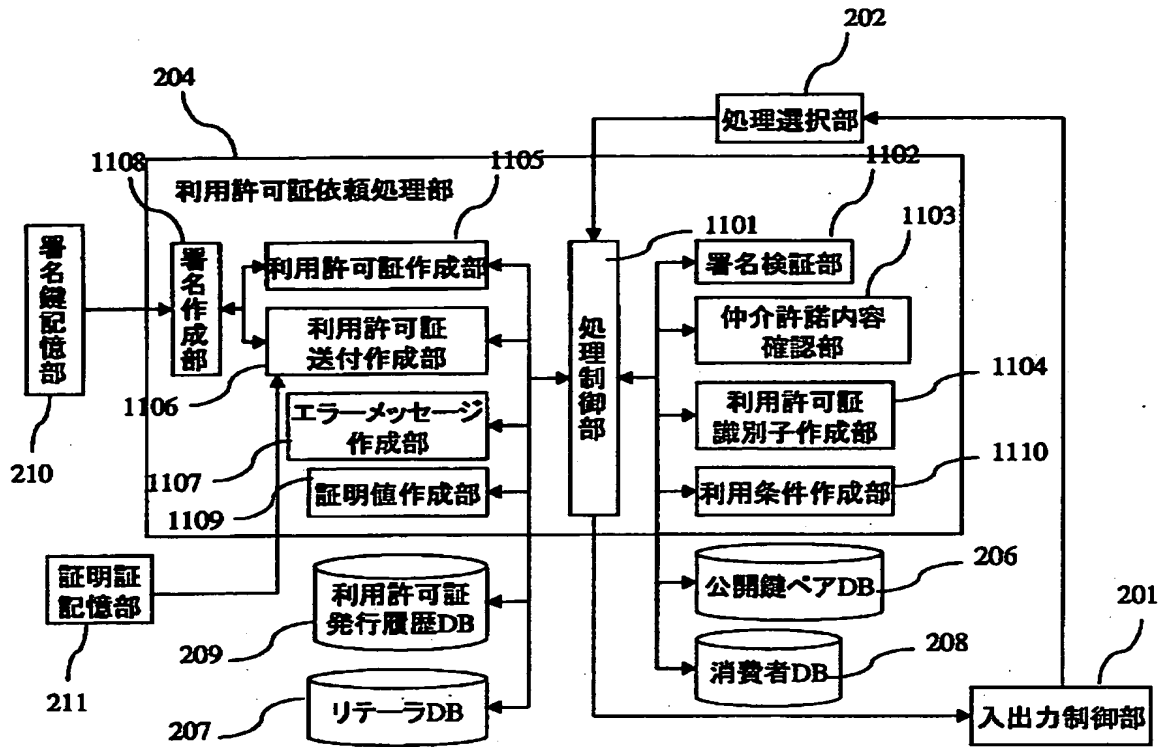
| 消費者識別子   | 消費者秘密情報  |
|----------|----------|
| CNS10001 | 10110... |
| CNS10002 | 11000... |
| CNS10003 | 01110... |
| ...      | ...      |

【図 1 0】

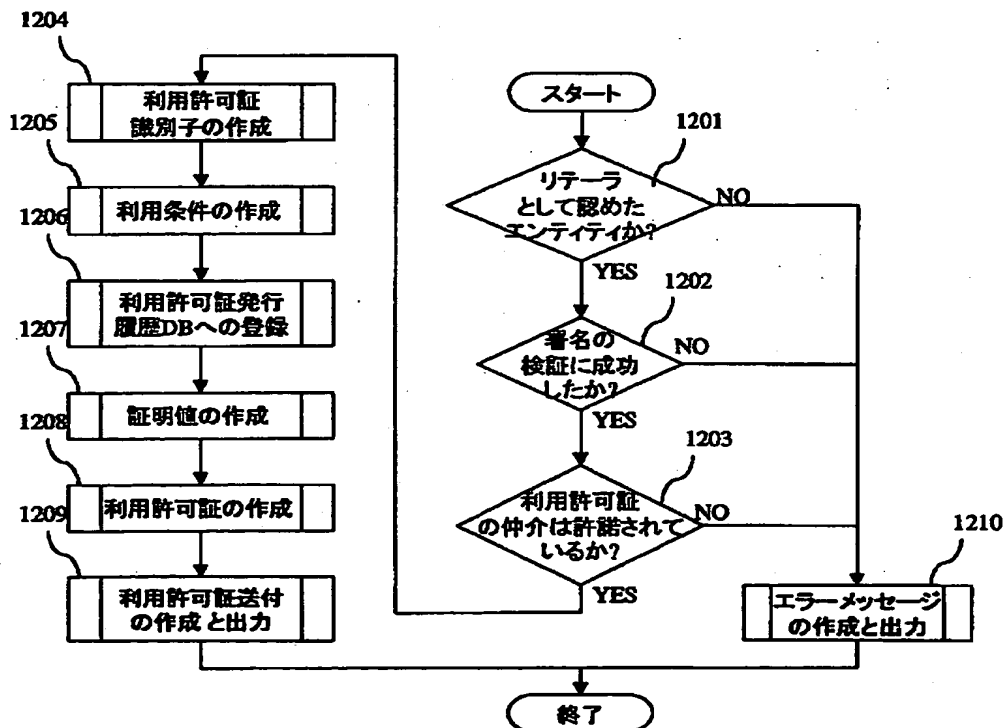
| 公開鍵識別子  | プロバイダ識別子 | 消費者識別子   | 仲介者識別子   | 利用条件     | 発行日        |
|---------|----------|----------|----------|----------|------------|
| PK00001 | PRV10001 | CNS10001 | RTL10002 | 2F34A... | 2000.2.1   |
| PK00002 | PRV10003 | CNS10001 | RTL10002 | 44FBC... | 1999.4.16  |
| PK00002 | PRV10003 | CNS10003 | RTL10001 | 5AAB1... | 1999.11.12 |
| ...     | ...      | ...      | ...      | ...      | ...        |



【図 1 1】

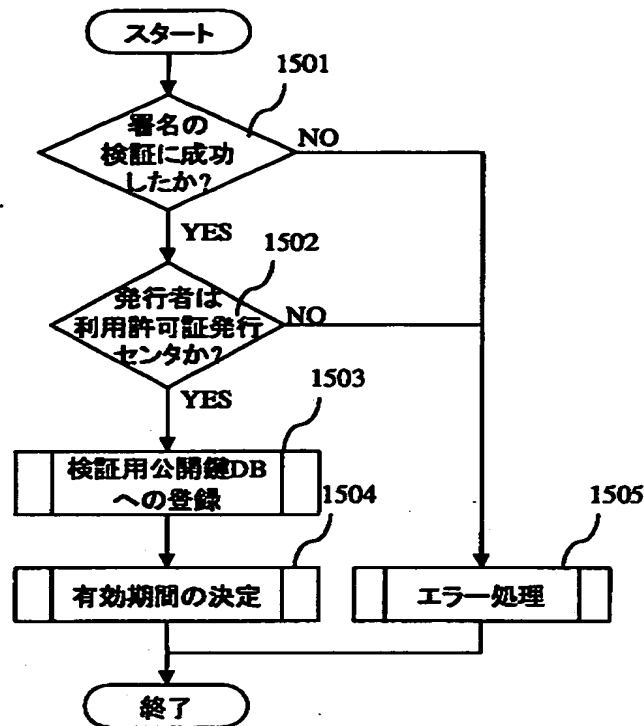


【図 1 2】

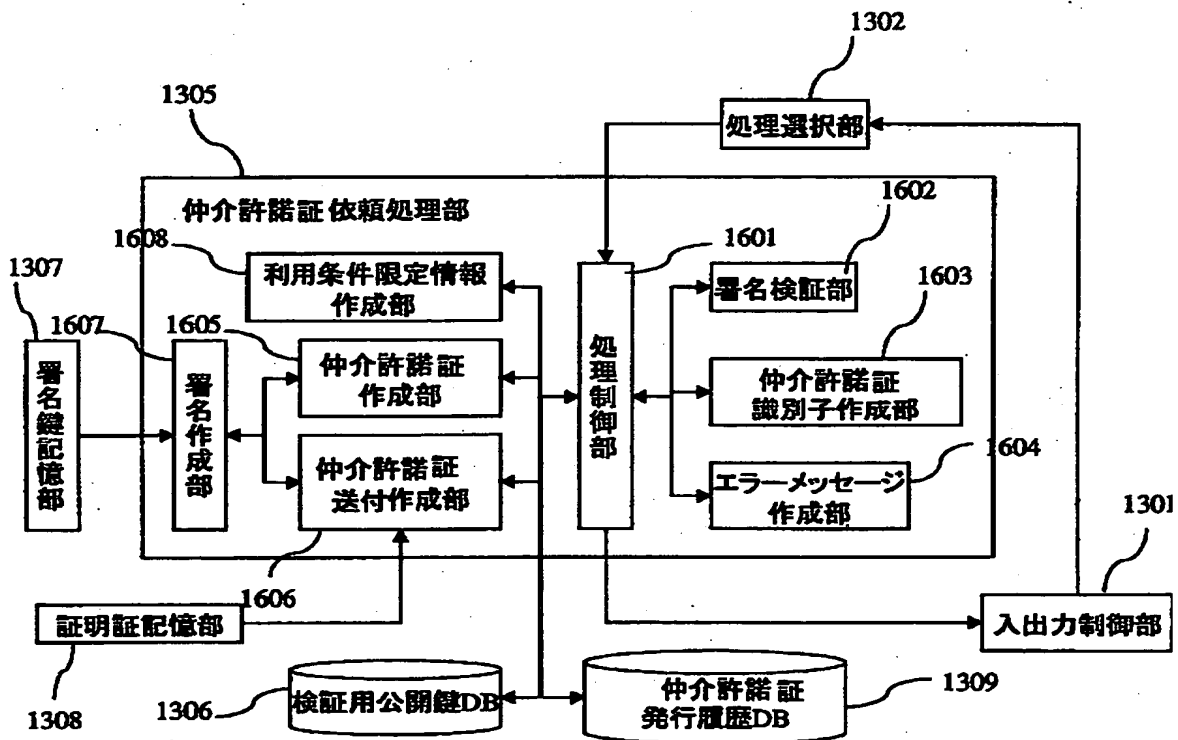




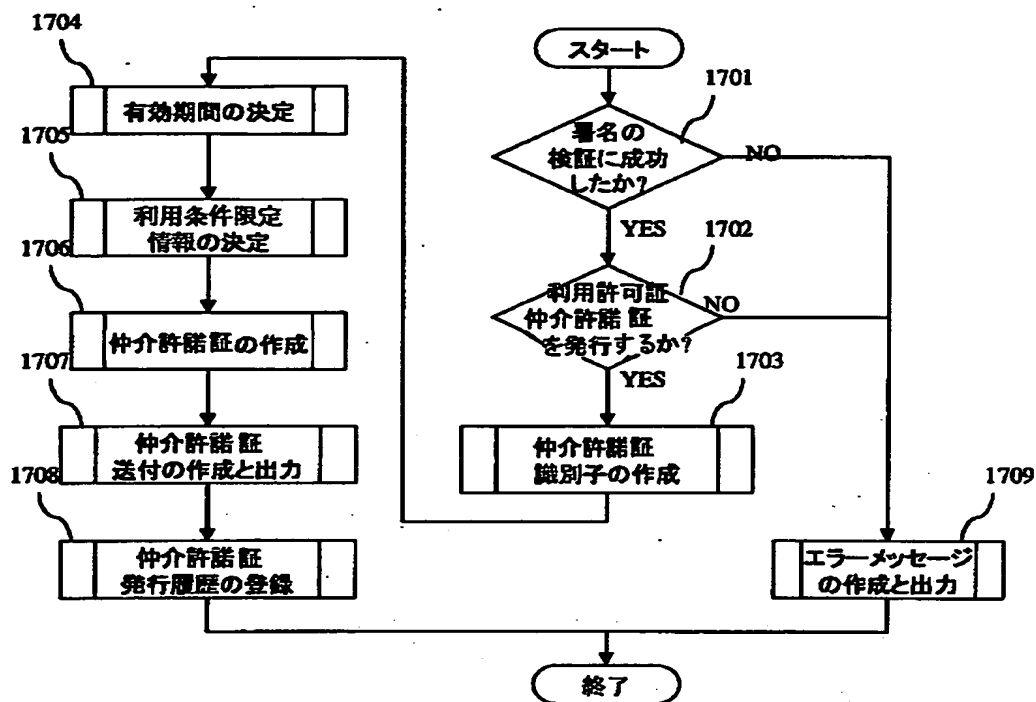
【図 15】



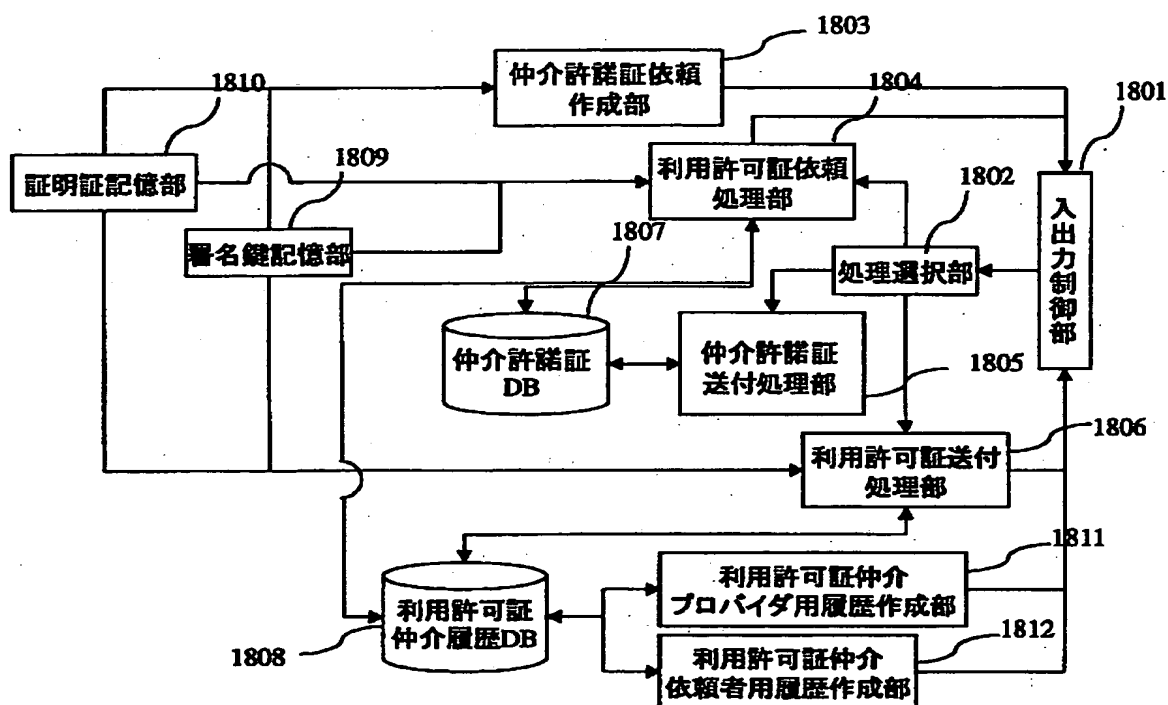
【図 16】



【图 17】



【图 18】



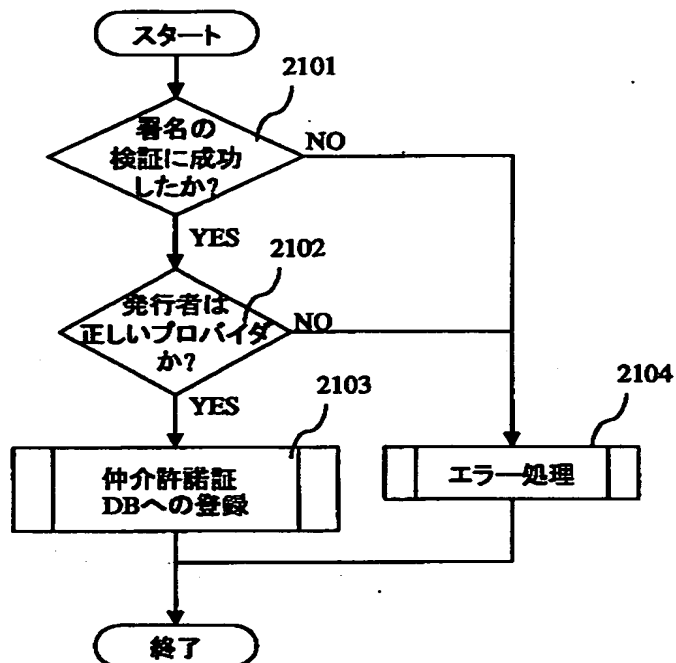
【図 1 9】

| 仲介許諾証 識別子 | 公開鍵識別子  | プロバイダ識別子 | 仲介許諾証     | プロバイダ証明証 |
|-----------|---------|----------|-----------|----------|
| AGM01002  | PK00001 | PRV10001 | FF3AC4... | FE66B... |
| AGM03010  | PK00002 | PRV10003 | FF3CC2... | FEE4A... |
| AGM03034  | PK00008 | PRV10003 | FFF87A... | FE7DE... |
| ...       | ...     | ...      | ...       | ...      |

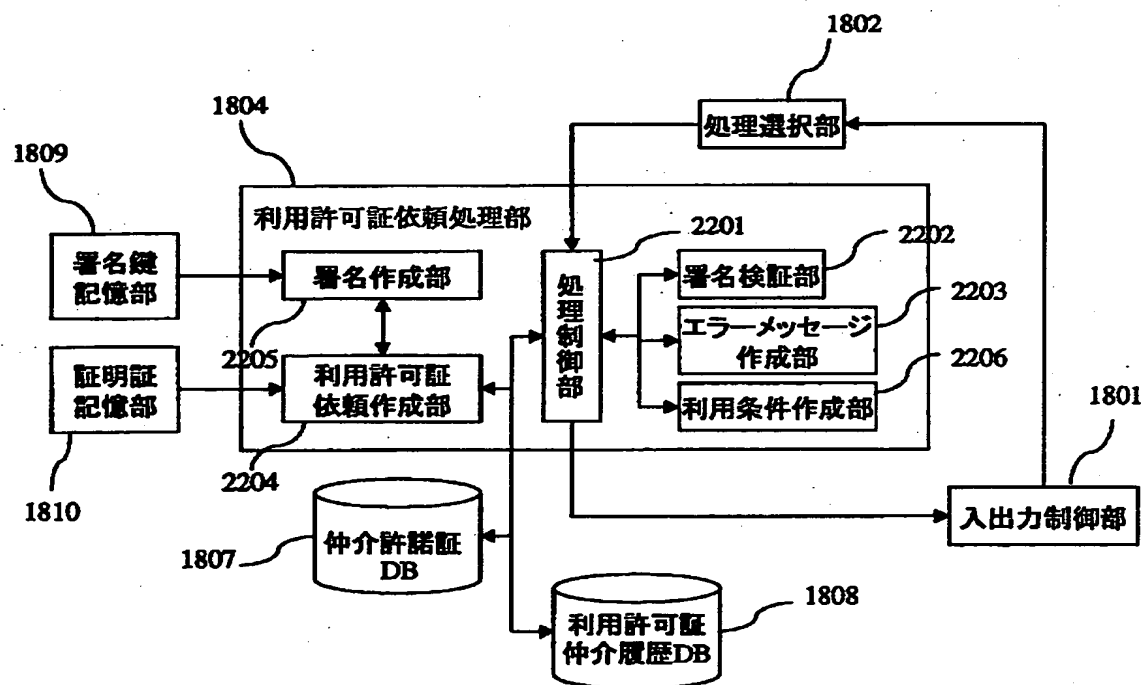
【図 2 0】

| 利用許可証<br>識別子 | 公開鍵<br>識別子 | プロバイダ<br>識別子 | 消費者<br>識別子 | 依頼者<br>識別子 | 利用条件     | 依頼日時               | 発信日時               |
|--------------|------------|--------------|------------|------------|----------|--------------------|--------------------|
| TKT10004     | PK00001    | PRV10001     | CNS10006   | CNS10006   | 2F34A... | 2000.2.1<br>10:25  | 2000.2.1<br>10:27  |
| TKT10010     | PK00008    | PRV10003     | CNS10003   | RTL10024   | 44FBC... | 2000.2.16<br>18:03 | 2000.2.16<br>18:04 |
|              | PK00001    | PRV10001     | CNS10012   | CNS10012   | 5AAB1... | 2000.3. 1<br>03:54 |                    |
| ...          | ...        | ...          | ...        |            | ...      | ...                | ...                |

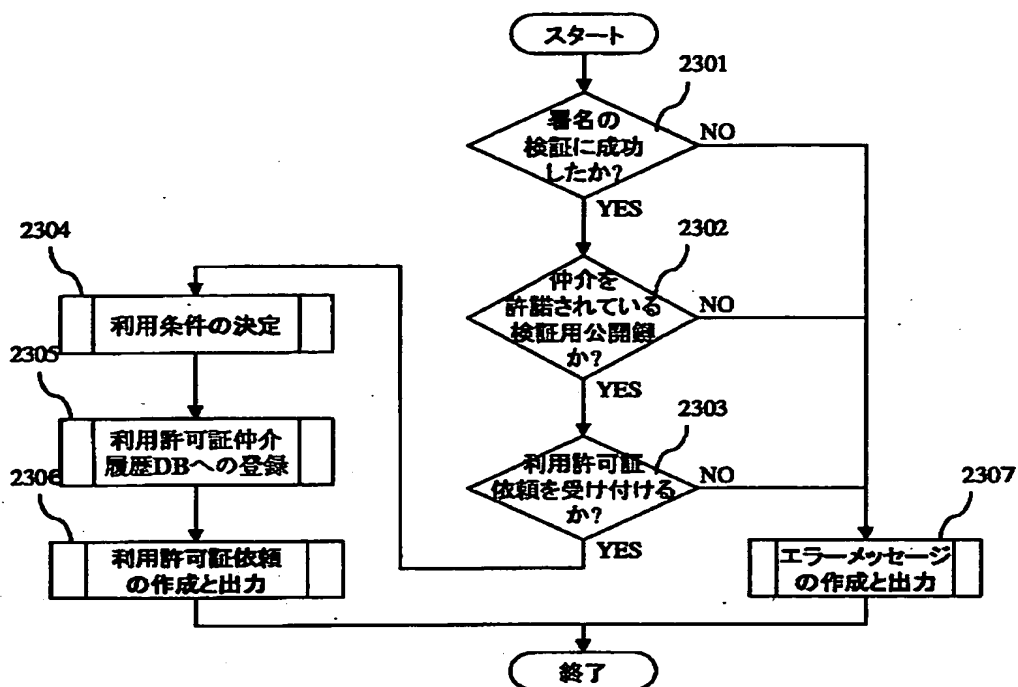
【図 2 1】



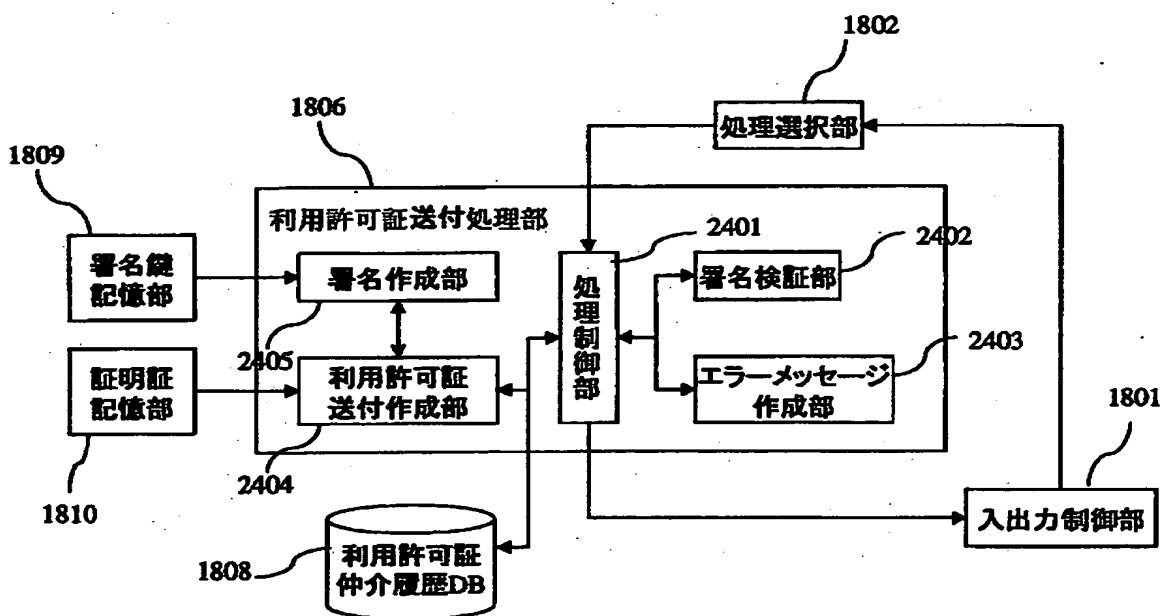
【图 2 2】



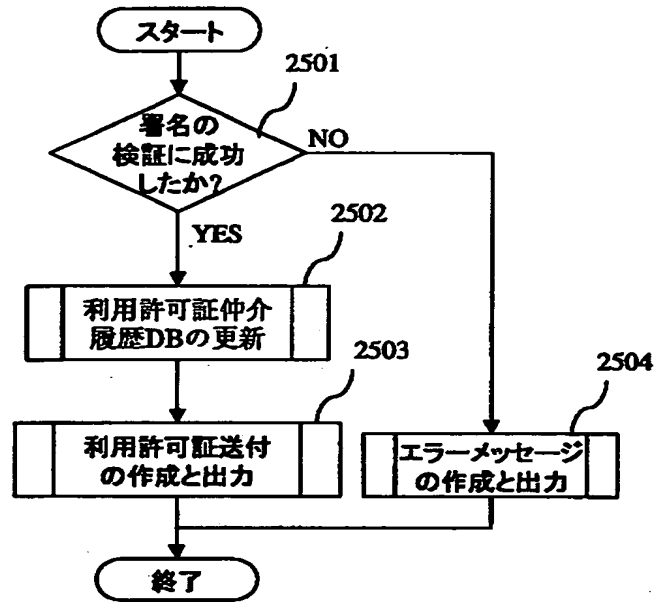
【図 2 3】



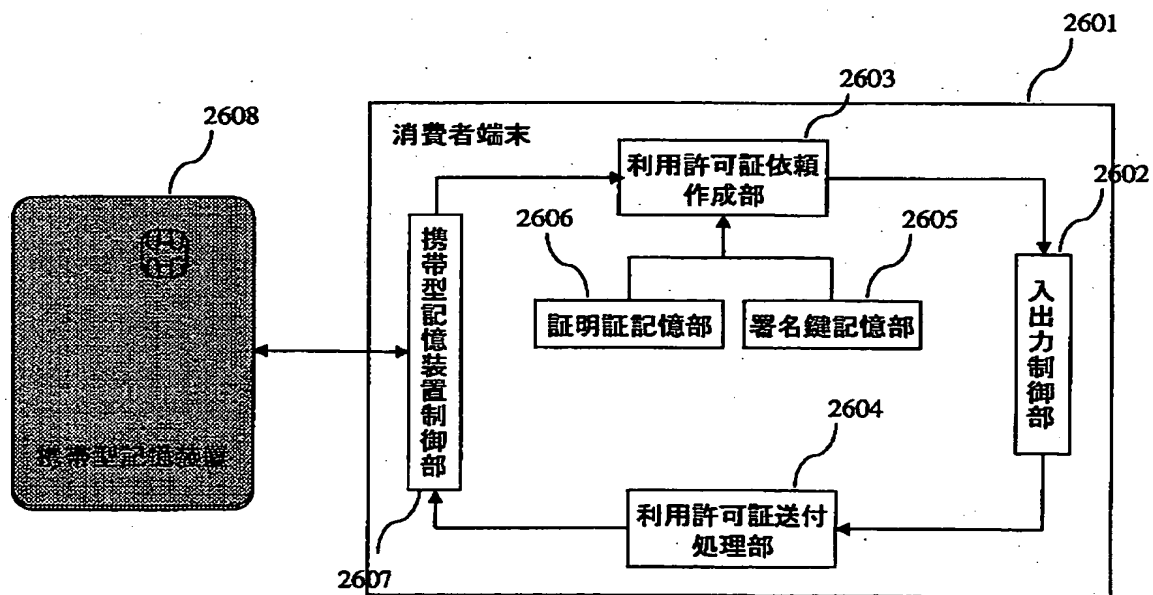
【図 2 4】



【図 25】

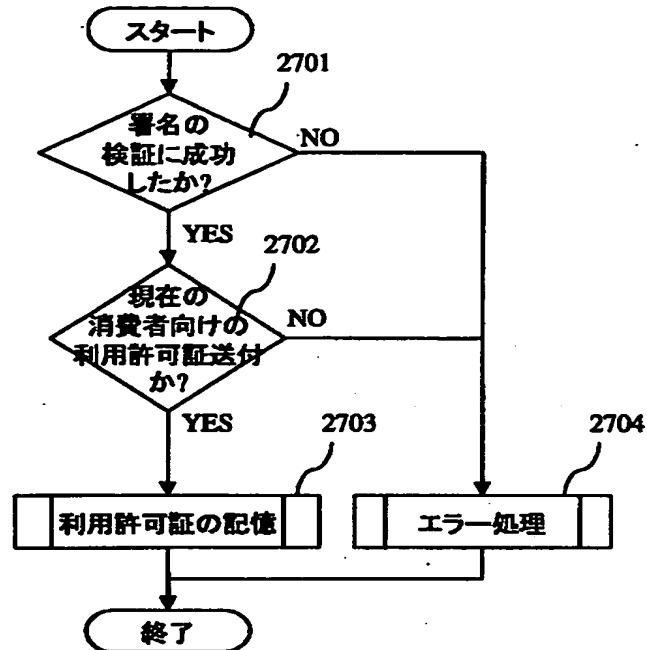


【図 26】

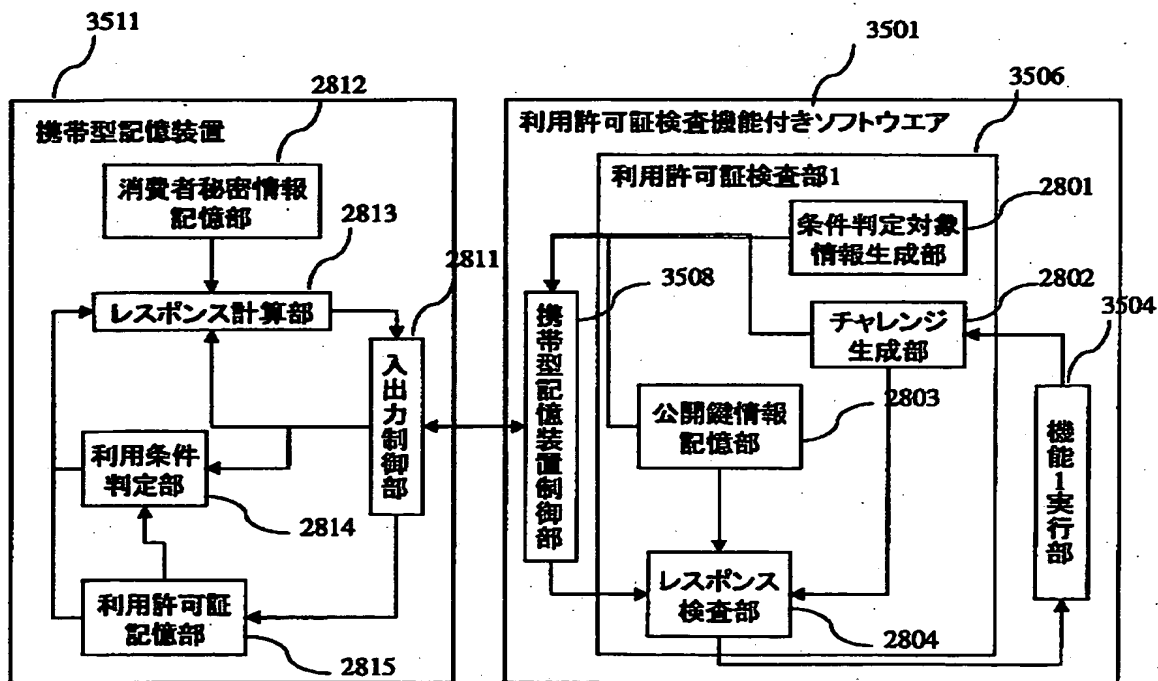




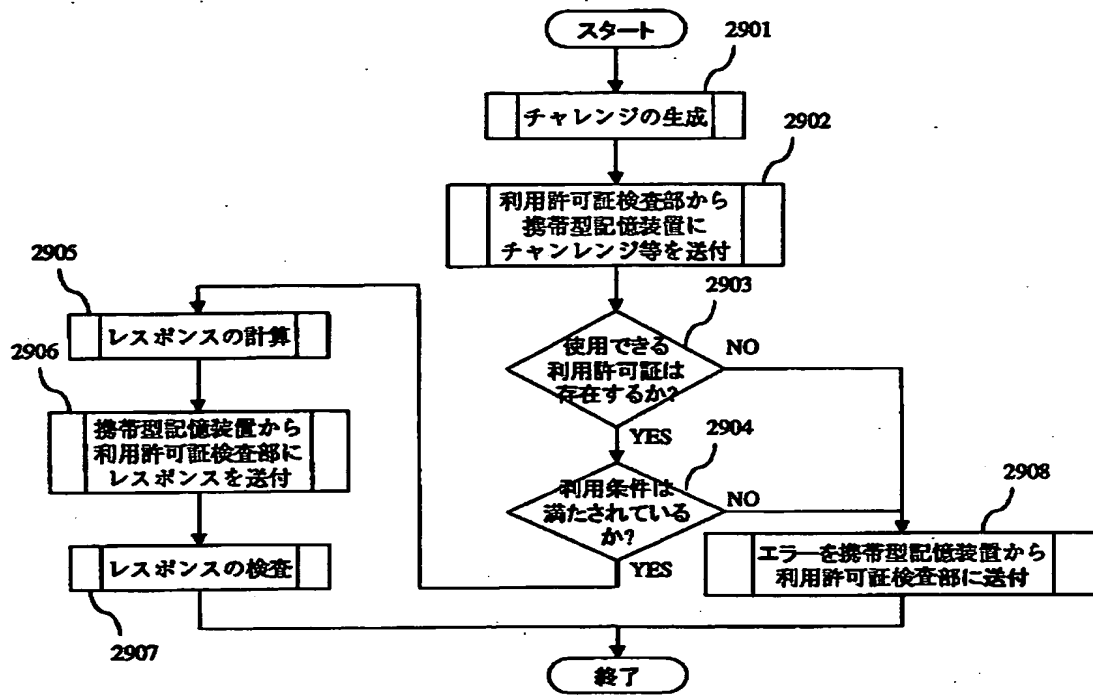
【図 27】



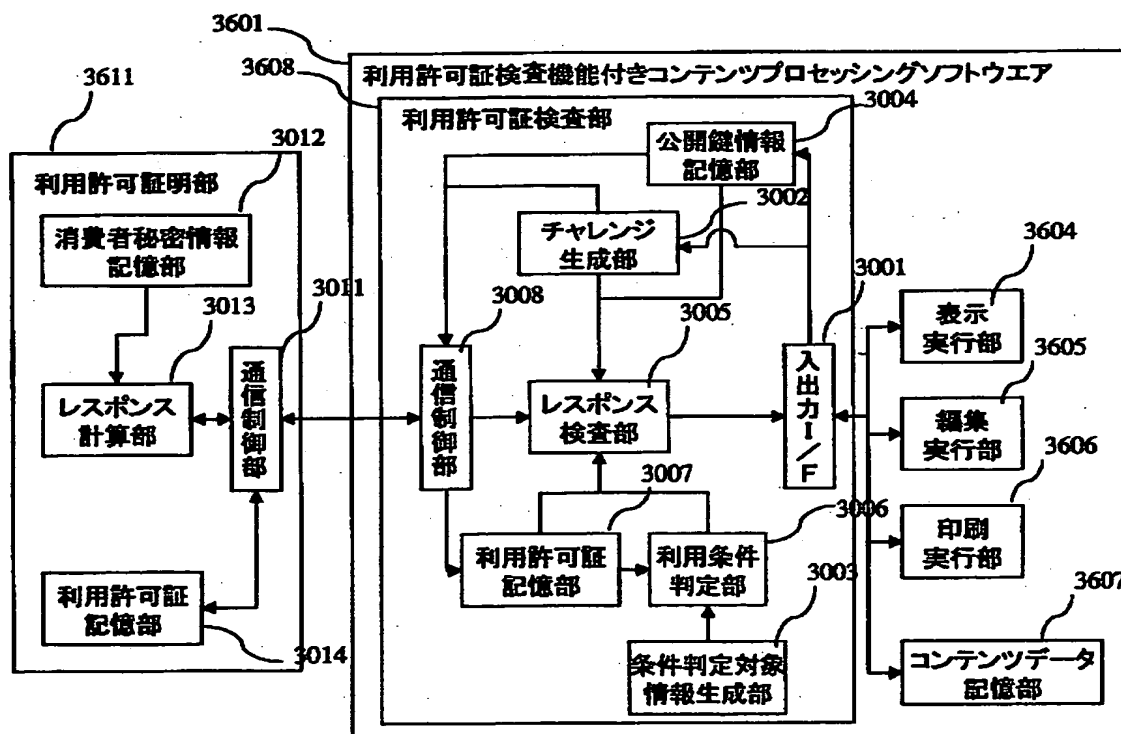
【図 28】



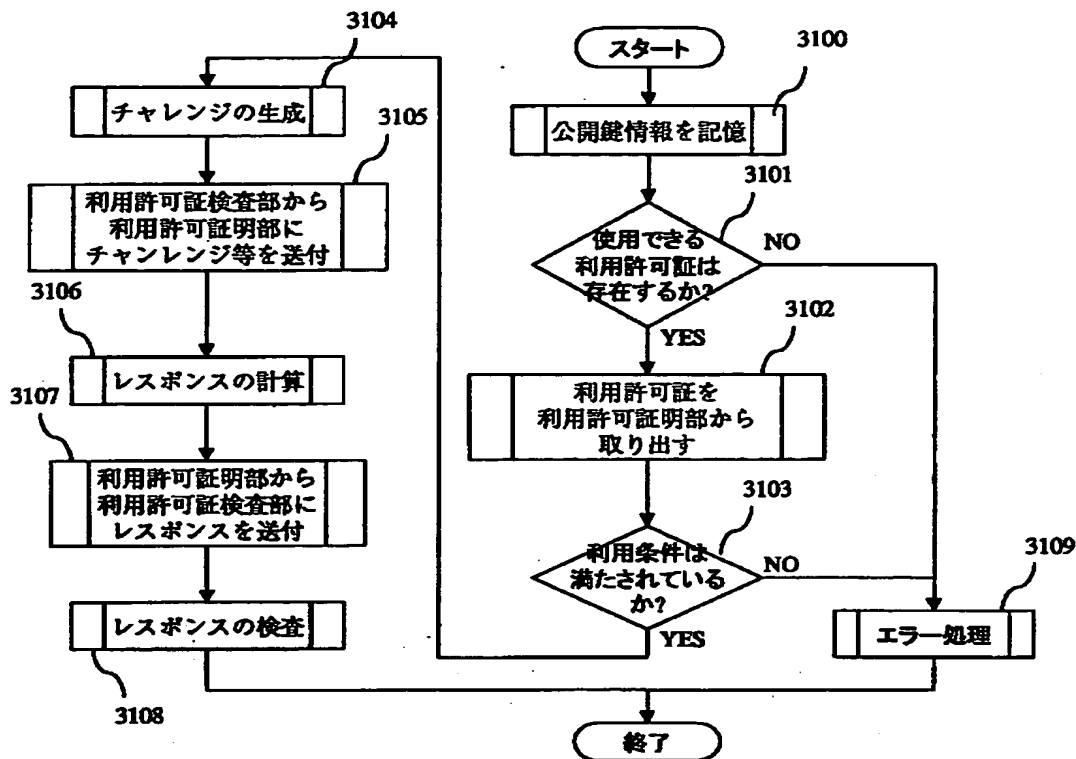
【図 29】



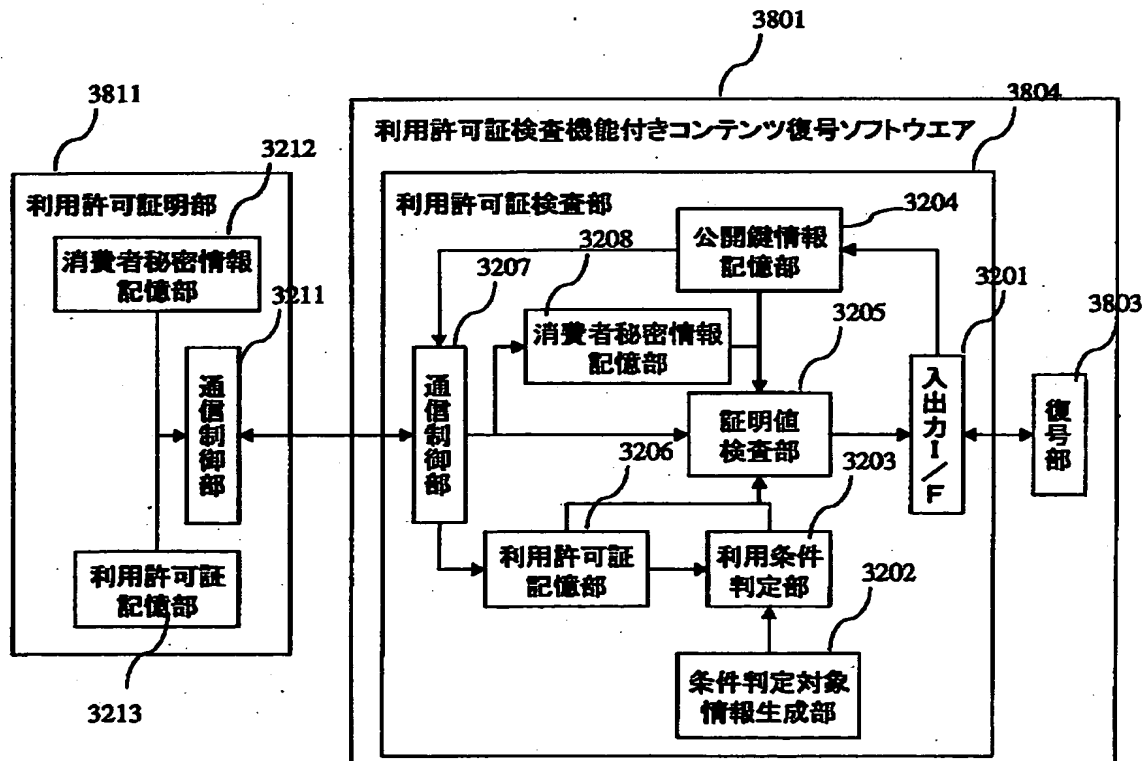
【図 30】



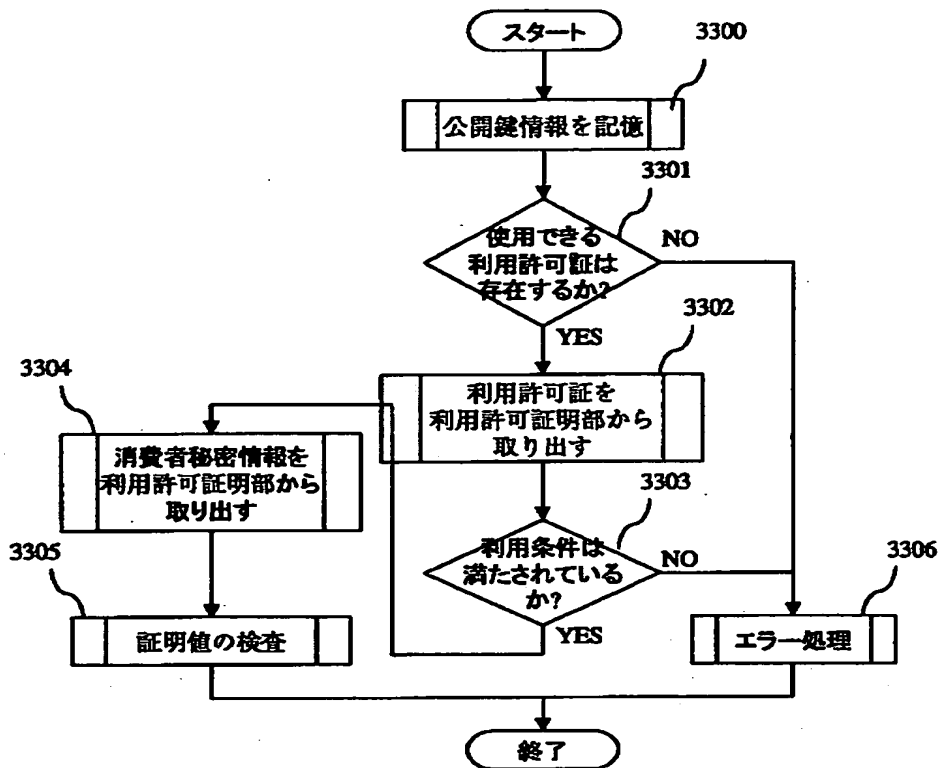
【図 3 1】



【図 3 2】



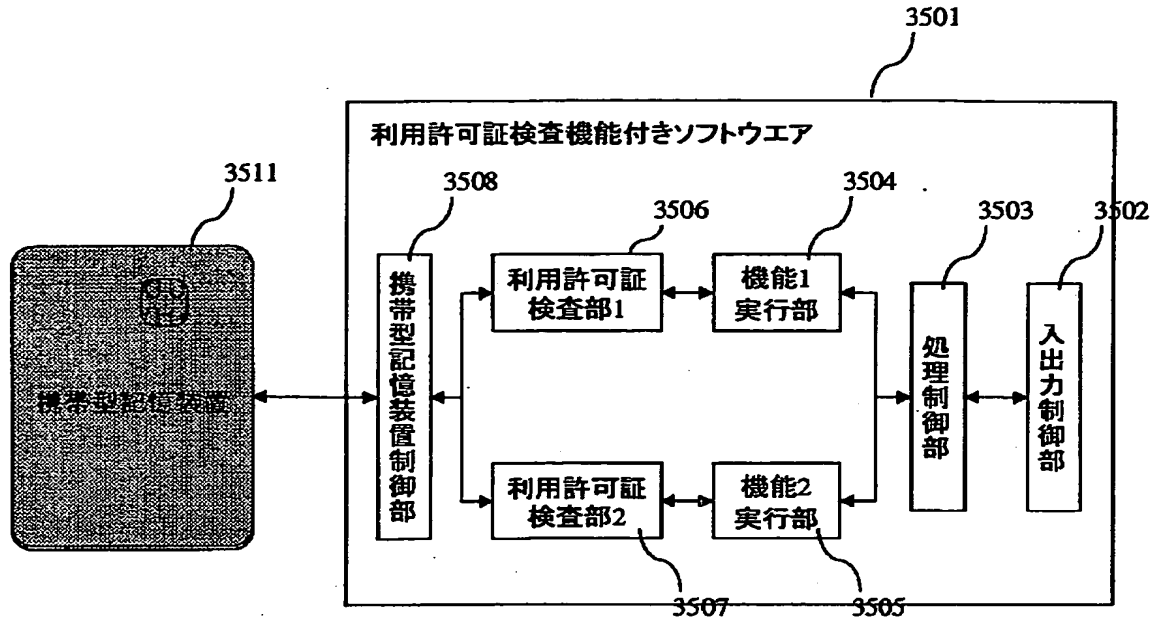
【図 3 3】



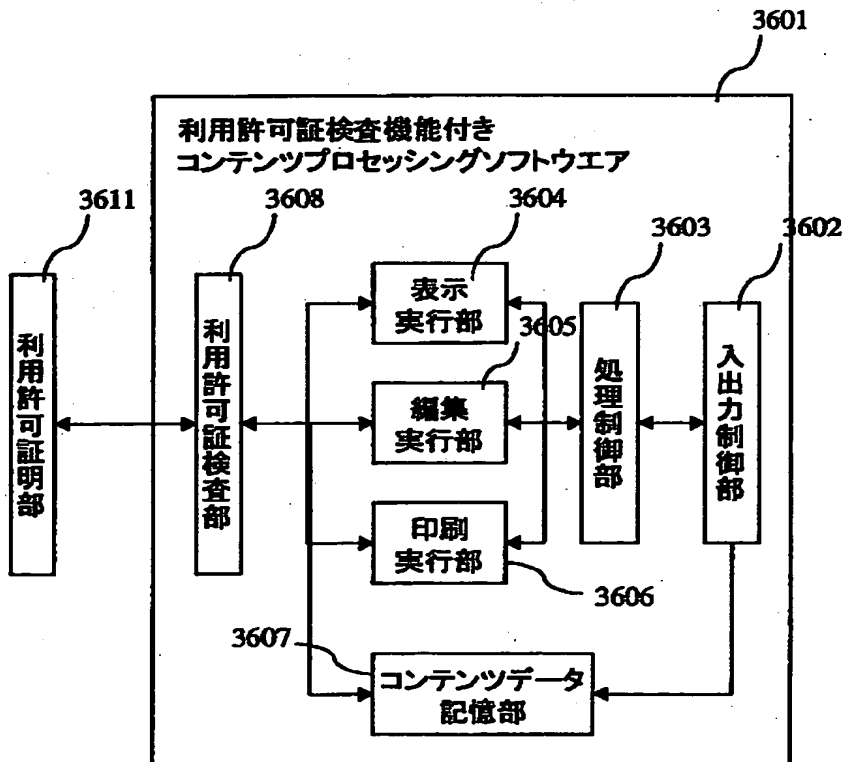
【図 3 4】

| 利用許可証仲介<br>許諾証識別子 | 公開鍵<br>識別子 | リテラ<br>識別子 | 利用条件<br>限定情報 | 有効期間<br>開始 | 有効期間<br>終了 | 発行日       |
|-------------------|------------|------------|--------------|------------|------------|-----------|
| AGM01002          | PK00001    | RTL10001   | FF3AC4...    | 1999.12.1  | 2000.11.31 | 1999.12.1 |
| AGM03010          | PK00002    | RTL10003   | FF3CC2...    | 2000.1.1   | 2000.7.1   | 2000.1.1  |
| AGM03034          | PK00008    | RTL10003   | FFF87A...    | 2000.3.4   | 2001.3.4   | 2000.3.3  |
| ...               | ...        | ...        | ...          | ...        | ...        | ...       |

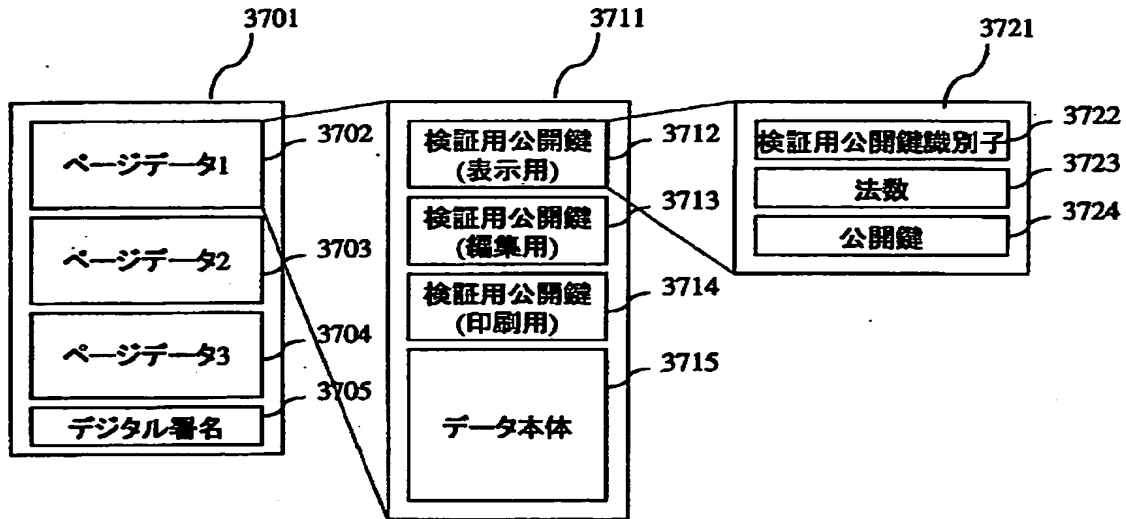
【図 3 5】



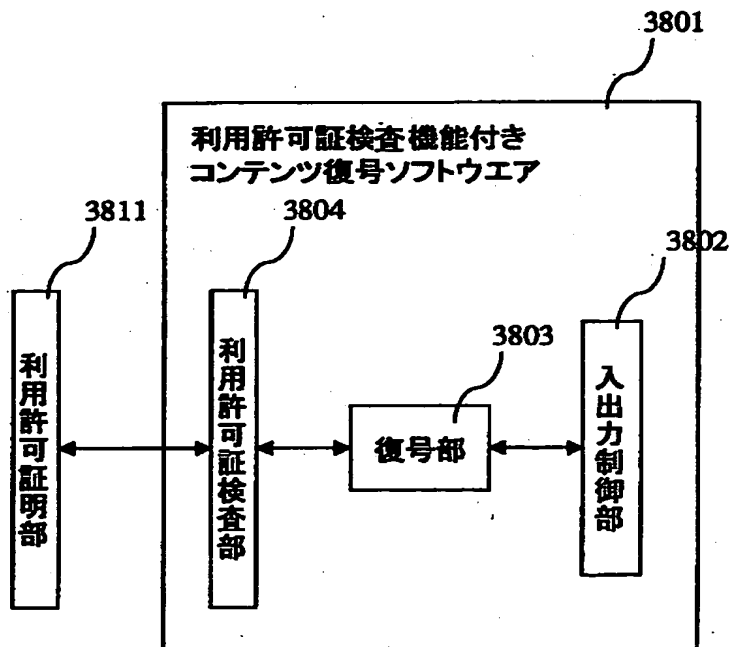
【図 3 6】



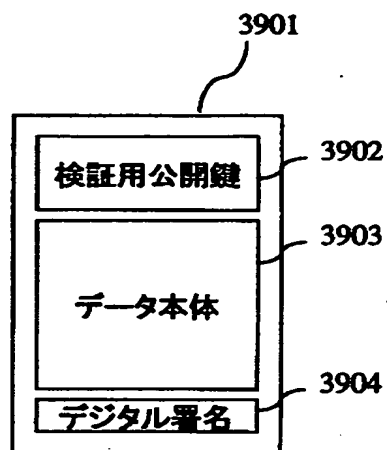
【図 3 7】



【図 3 8】



【図 3 9】



【書類名】 要約書

【要約】

【課題】 デジタルコンテンツ提供者、販売者が自らのリソースを消費することなく利用許可証を消費者に発行できるようにする。

【解決手段】 リテーラ 1 0 3 は消費者端末 1 0 9 にインターネット 1 0 1 を介してデジタルコンテンツを販売する。リテーラ 1 0 3 はデジタルコンテンツおよび購入者に応じた利用許可証の発行を利用許可証発行センタ 1 0 2 に要求して利用許可証を受領する。消費者端末 1 0 9 はリテーラ 1 0 3 からインターネット 1 0 1 を介して利用許可証を受け取る。消費者はプロバイダ 1 0 5 から提供を受けたデジタルコンテンツを利用する際に、利用許可証を用いて正規の購入者であることを証明する。証明が成功裏に検証されたときに、消費者はデジタルコンテンツを利用できるようになる。

【選択図】 図 1



出 願 人 履 歴 情 報

識別番号 [000005496]

1. 変更年月日 1996年 5月29日  
[変更理由] 住所変更  
住 所 東京都港区赤坂二丁目17番22号  
氏 名 富士ゼロックス株式会社